Recipe 19 - Configuration Guide for Setting up RSA Federated Identity Manager 2.5LA as an AA and CS

Table of Contents:

Version 2.0.0

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and RSA Federated Identity Manger v2.5LA as an Agency Application (AA) and Credential Service (CS). Remember that the RSA Federated Identity Manager setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0 starting with RSA ClearTrust System Configuration.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

2 Partner Configuration

2.1 RSA ClearTrust System Configuration

Before configuring RSA Federated Identity Manger as an AA or CS, be sure that the system is properly configured by using RSA ClearTrust. With the administration Graphical User Interface (GUI) servlet container running (generally Tomcat) open a web browser (i.e. Internet Explorer) and go to http://localhost:8080/admingui/index.jsp. Login to RSA ClearTrust with administration privileges and follow the instructions provided below.

First, verify that the server has been defined, as well as an application with the appropriate resources. From the RSA ClearTrust home screen, click on **Define Resources > Applications > Manage Existing**, which is demonstrated in Figure 19-1. Applications can be viewed and edited by selecting an application and clicking on **Edit,** which is found in the Edit column of the Applications table. New applications can be added by clicking on the **Add New** button provided above the Applications table.

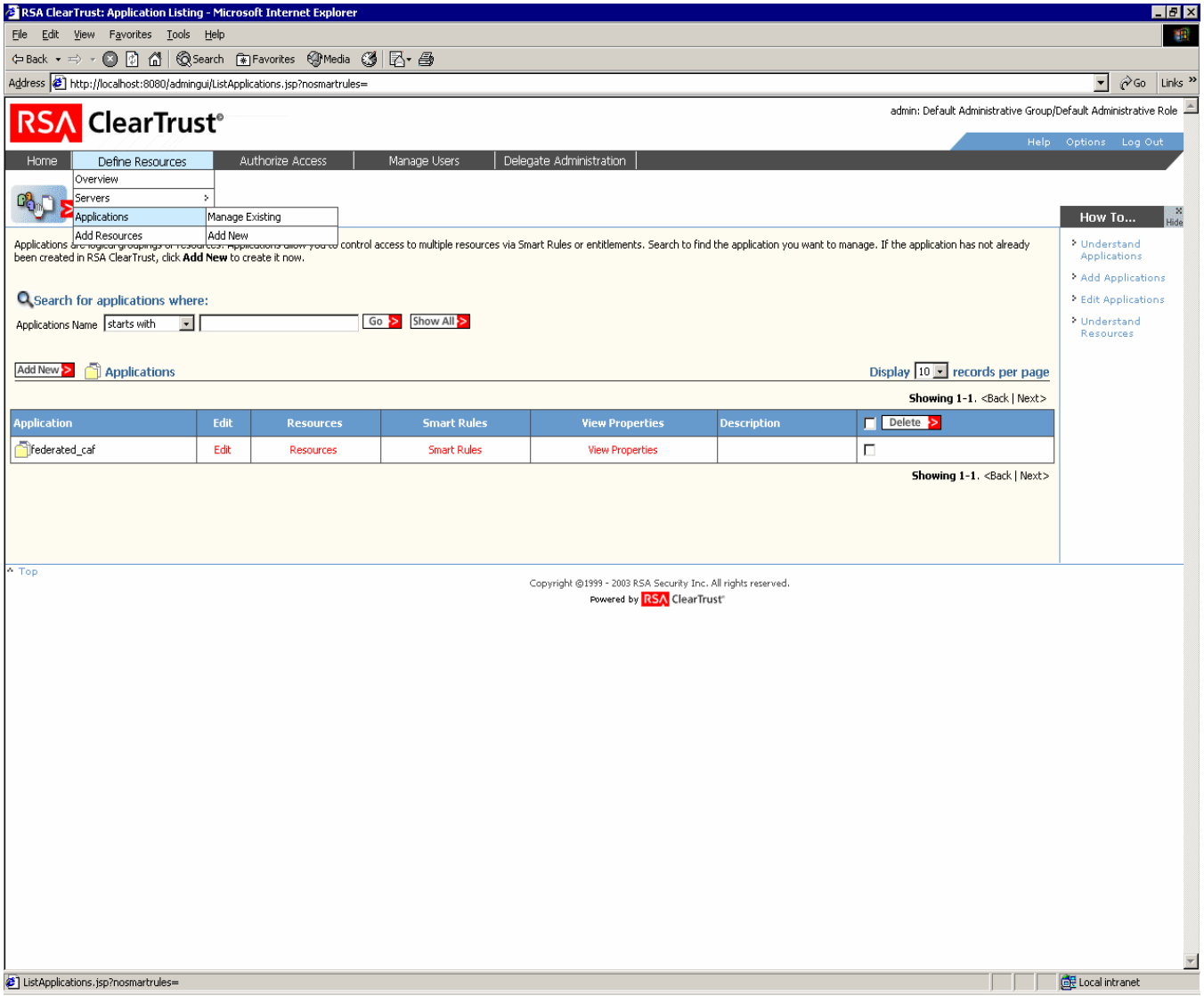

Figure 19-1: Server Verification

Next, verify that users are present and have entitlements to the web application. This is done by clicking on **Manage Users > Users** & **Administrators**. The Users & Administrators screen will appear as shown in Figure 19-2. Users can be viewed and edited by selecting a user and clicking on **Edit,** which is found in the Edit column of the Users table. New users can be added by clicking on the **Add New** button provided above the Users table.

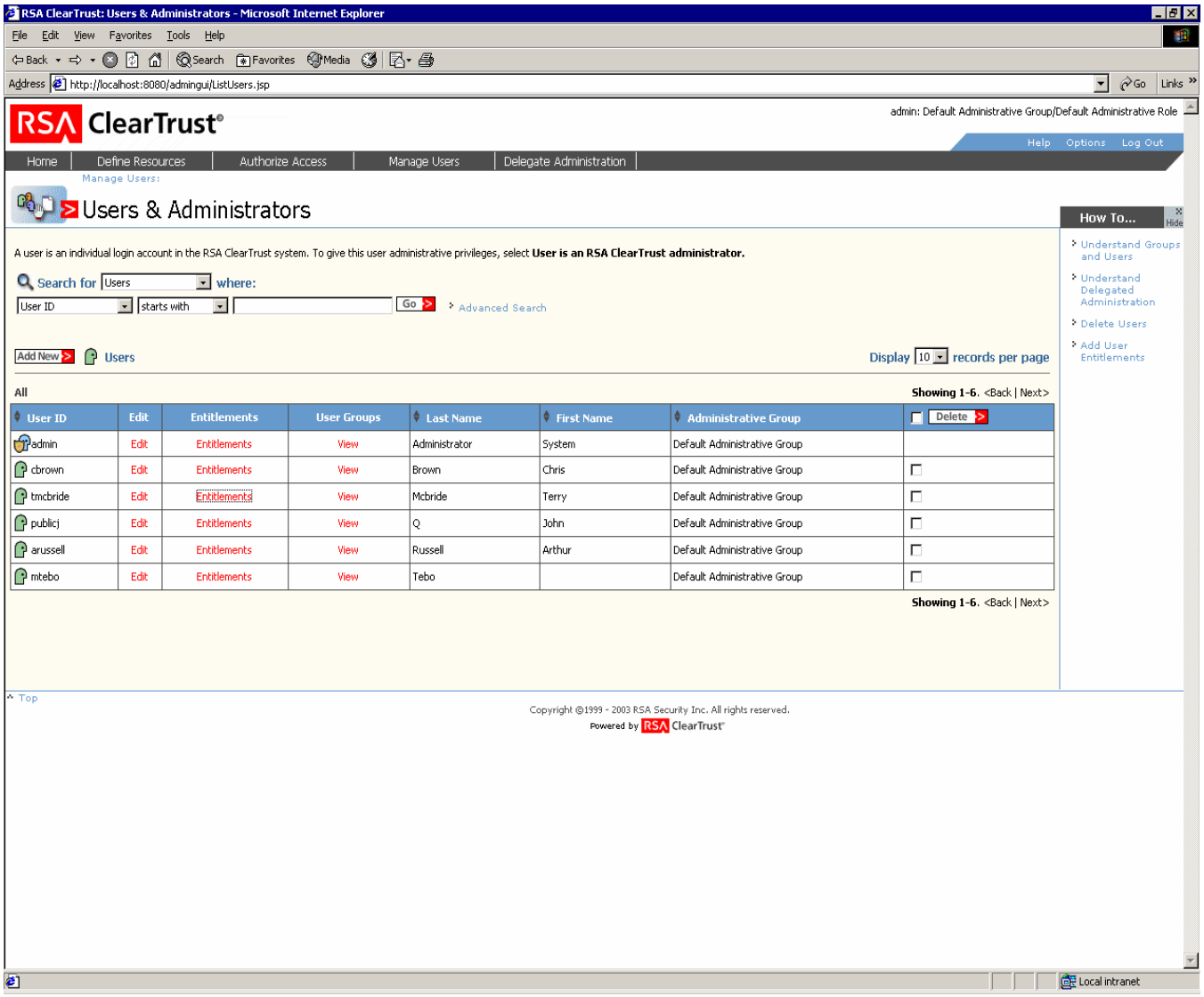

Figure 19-2: Users & Administrators

After verifying users are present, make sure properties corresponding to the user's attributes you wish to send/receive using SAML assertions have been added. Some properties require modification of the backend user store. This is done by clicking on **Manage Users > Properties**. The Properties screen will appear as shown in Figure 19-3. Properties can be viewed and edited by selecting a property and clicking on **Edit,** which is found in the Edit column of the Properties table. New properties can be added by clicking on the **Add New** button provided above the Properties table.

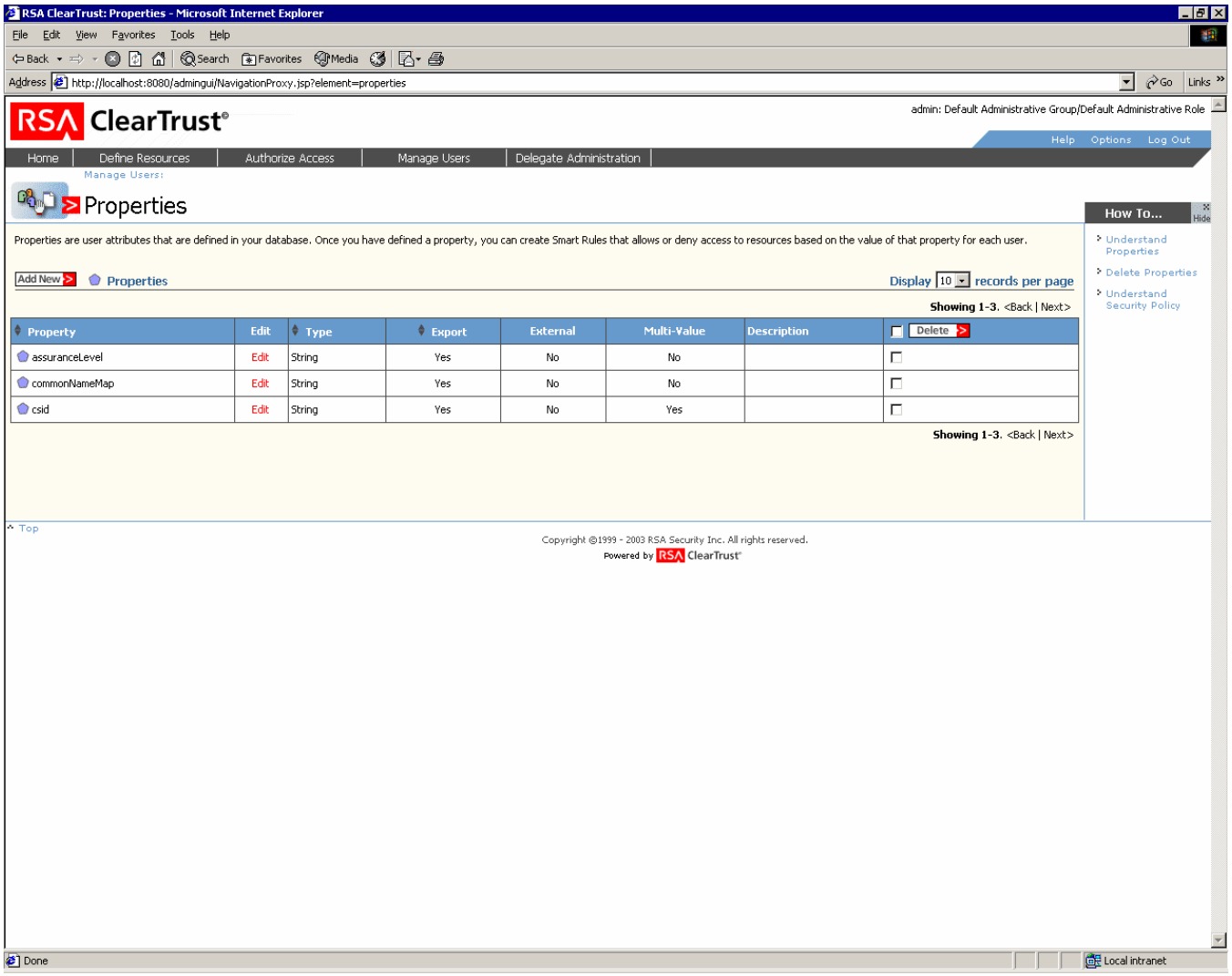

Figure 19-3: Properties

2.2 RSA Federated Identity Manager System Configuration

Next, in RSA Federated Identity Manager, verify attribute plug-ins are present and configured. To access RSA Federated Identity Manager, open a web browser (i.e. Internet Explorer), with the managed server running, go to http://e1-s3k4.caf.eauth.enspier.net:7001/samlconfig/Index.jsp, and then log-in with administration privileges.

Plug-ins map users attributes in ClearTrust to the SAML Assertion attributes and vice versa. For E-Authentication participants, plug-ins are available to enable support for required attributes. Please contact RSA for further information regarding plug-ins.

The attribute plug-in for a CS is **RSA SpecialCTAttributePluginAP**, and the attribute plug-in for an AA is **RSA SpecailCTAttributePluginRP**. Attribute plug-ins can be verified by clicking on **Configure System > Plug-Ins > Manage Existing**. The Plug-Ins screen will appear as shown in Figure 19-4. Attribute plug-ins can be viewed and edited by selecting a plug-in and clicking on **Edit,** which is found in the Edit column of the Plug-In table. Attribute plug-ins can be added by clicking on the **Add New** button provided above the Plug-in table.

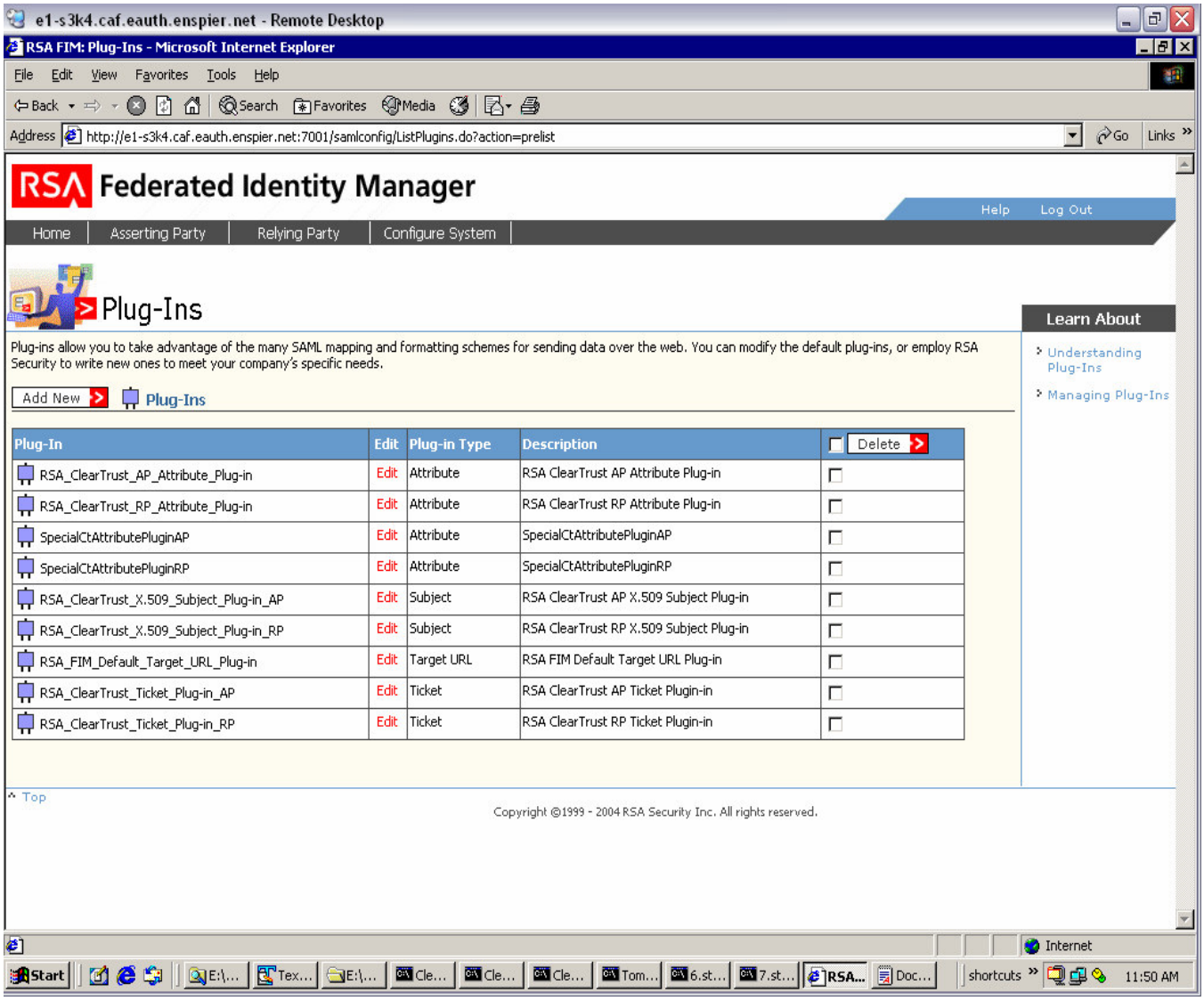

Figure 19-4: View Attribute Plug-Ins

Custom plug-ins are generally java classes that reside in <FIM Home>/rsaappserver/ext. A custom plug-in can be configured as demonstrated in Figure 19-5.

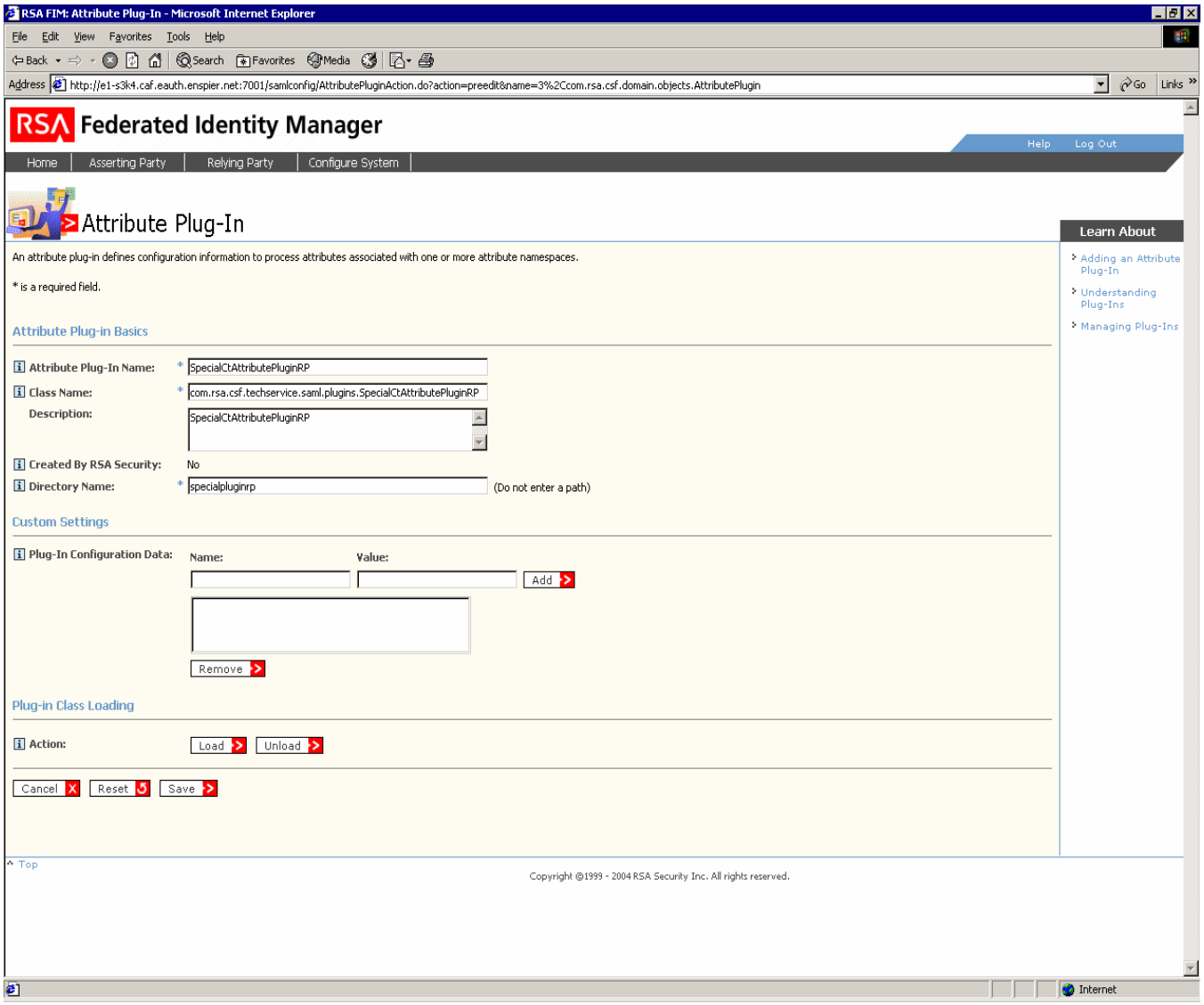

Figure 19-5: Attribute Plug-In

Next, from the Plug-Ins screen, verify that subject plug-ins are present and configured. These plug-ins map the local user to the subject of the assertion that is being sent and vice versa.

The subject plug-in for a CS is **RSA_ClearTrust_X.509_Subject_Plug-in_AP**, and the subject plug-in for an AAs is **RSA_ClearTrust_X.509_Subject_Plug-in_RP**. Subject plug-ins can be viewed and edited by selecting a plug-in and clicking on **Edit,** which is found in the Edit column of the Plug-In table. Subject plug-ins can be added by clicking on the **Add New** button provided above the Plug-In table.

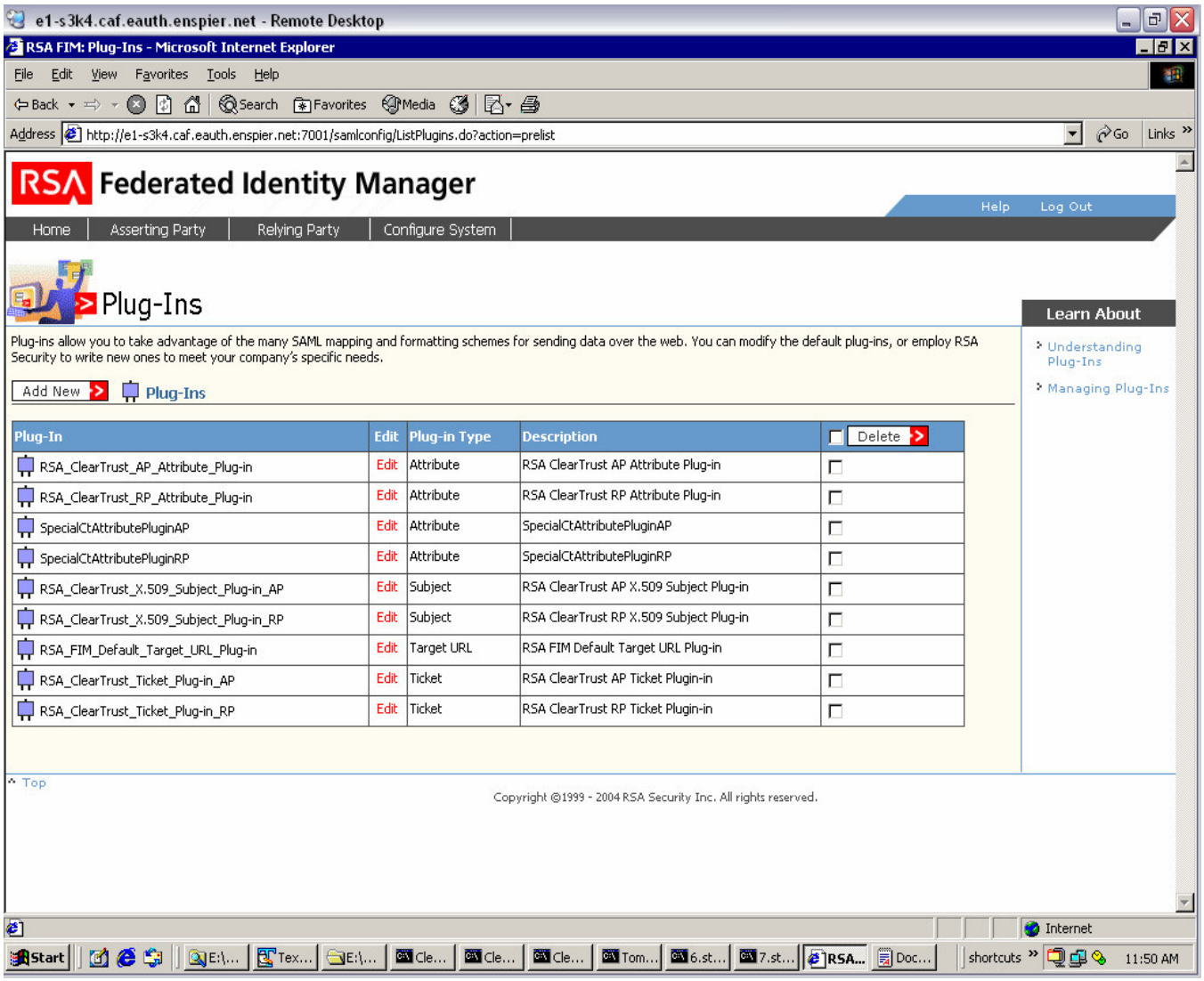

Figure 19-6: View Subject Plug-Ins

Figure 19-7 provides an example configuration for a subject plug-in for a CS. The Custom Settings section script maps the user's uid attribute from the LDAP directory to the subject of the assertion.

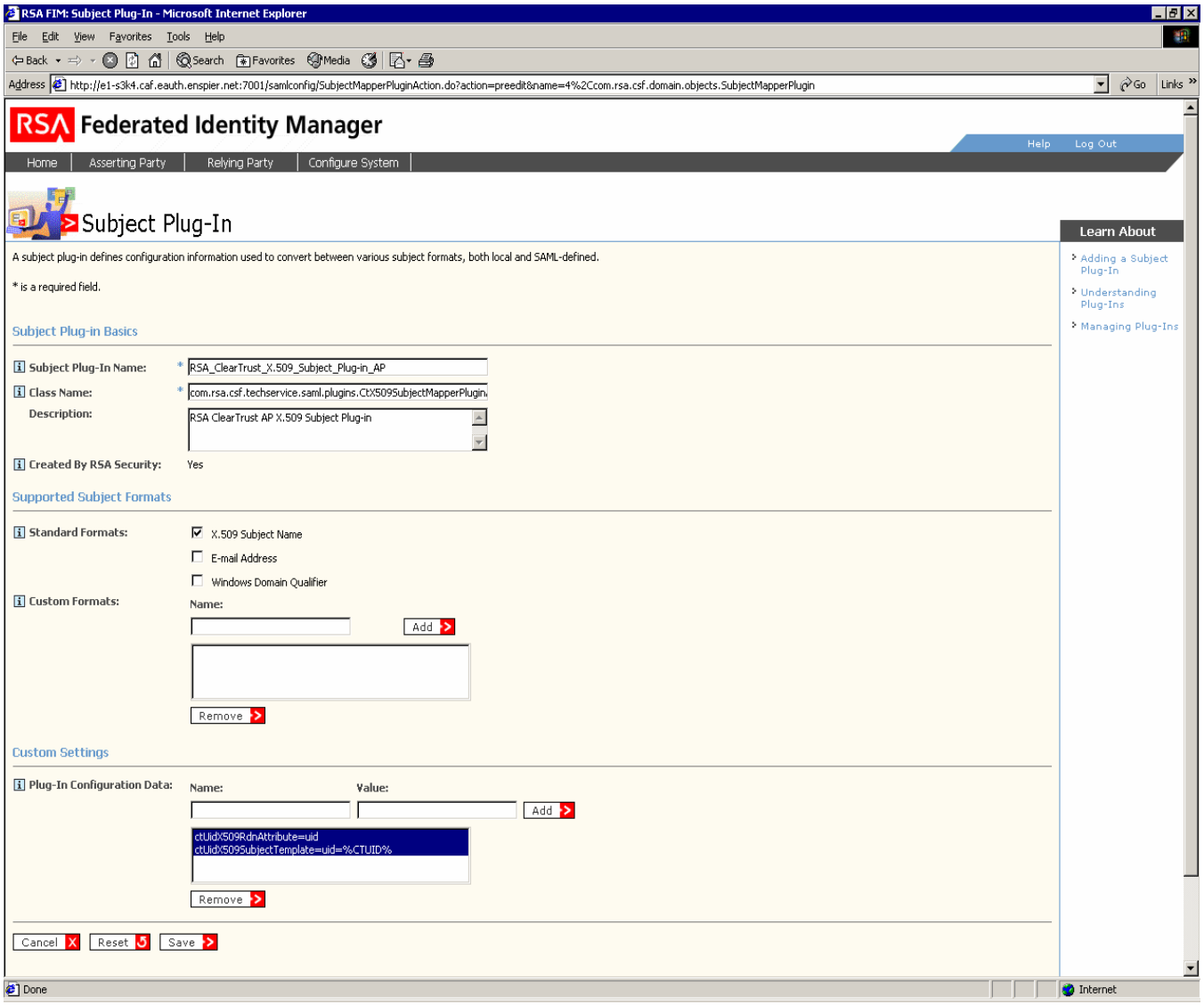

Figure 19-7: Subject Plug-In

Figure 19-8 provides an example configuration for a subject plug-in for an AA. The Custom Settings section script maps the subject of the assertion to the user's uid attribute from the LDAP directory.

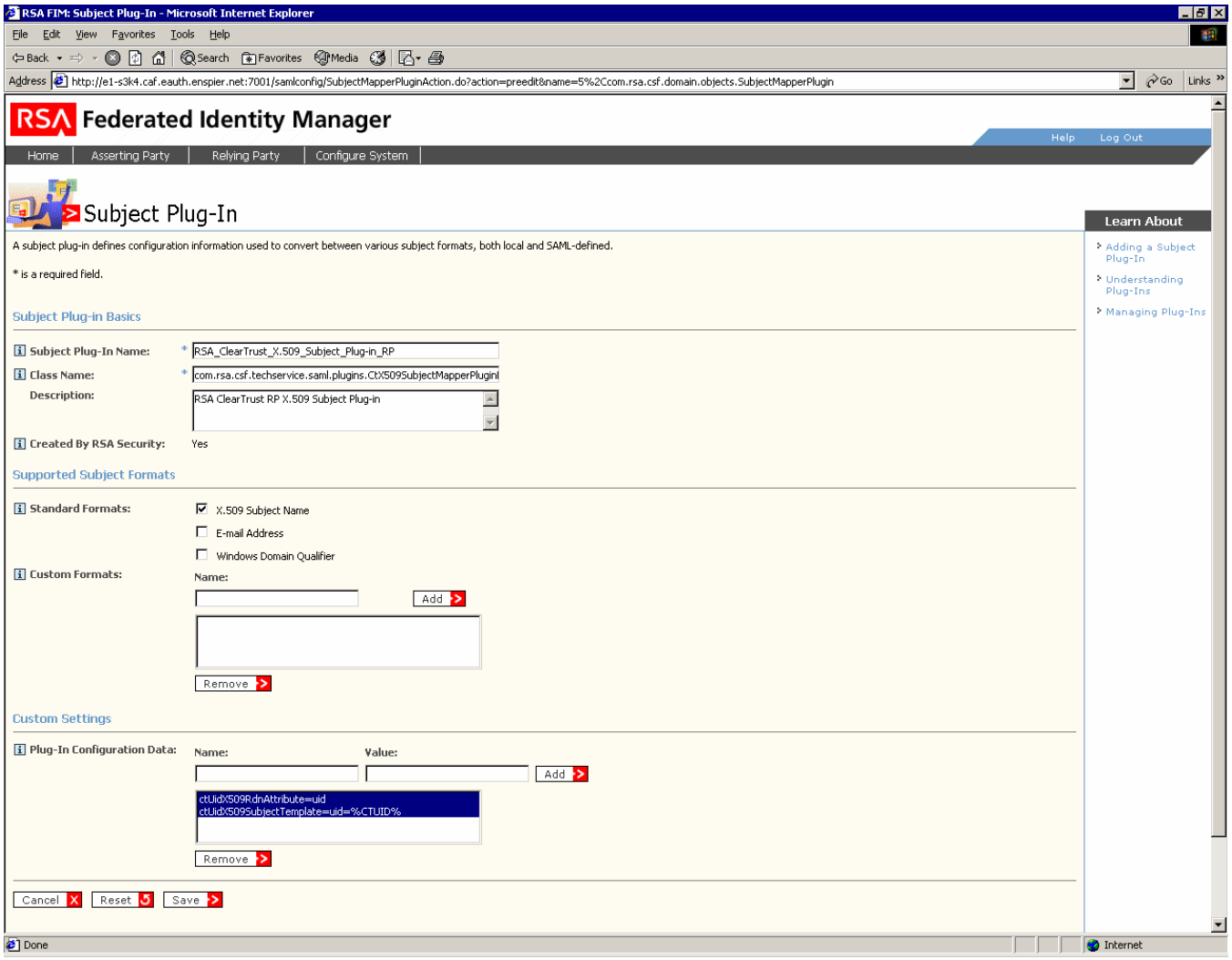

Figure 19-8: Example Subject Plug-In for an AA

Next, namespaces must be defined. CSs must define an attribute namespace to send in assertions. Currently E-Authentication requires this to be http://eauthentication.gsa.gov/federated/attribute. An AA must define subject namespaces that match the namequalifier attribute in the nameidentifier element of assertions received from SAML partners.

Namespaces can be defined by clicking on **Configure System > Namespaces > Manage Existing**. The Namespaces screen should appear as shown in Figure 19-9. Namespaces can be viewed and edited by selecting a namespace and clicking on **Edit,** which is found in the Edit column of the Namespaces table. New namespaces can be added by clicking on the **Add New** button provided above the Namespaces table.

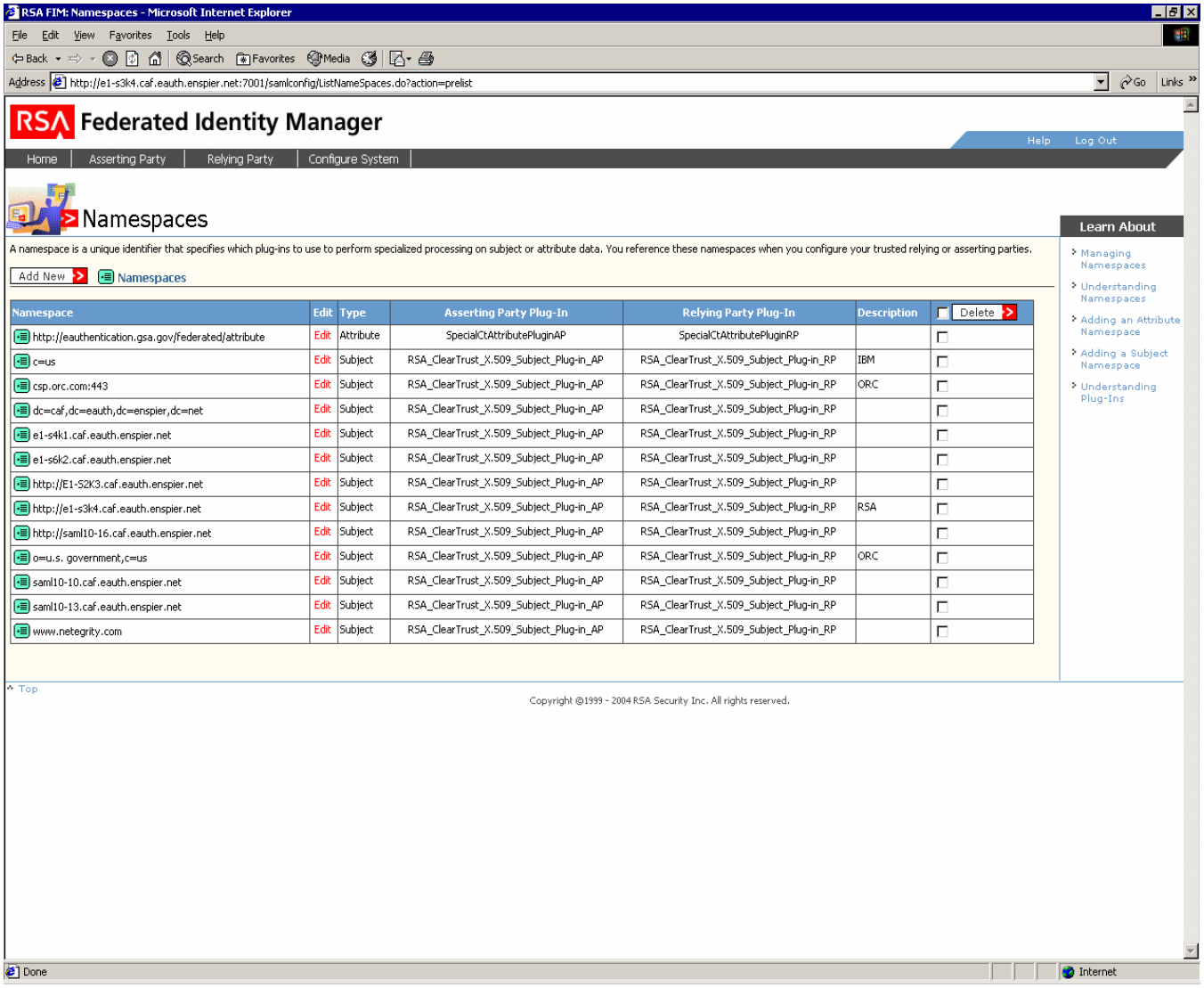

Figure 19-9: Namespaces

Figure 19-10 provides an example of how to configure an attribute namespace for a CS. Notice this is linked to the subject plug-in provided in the previous step.

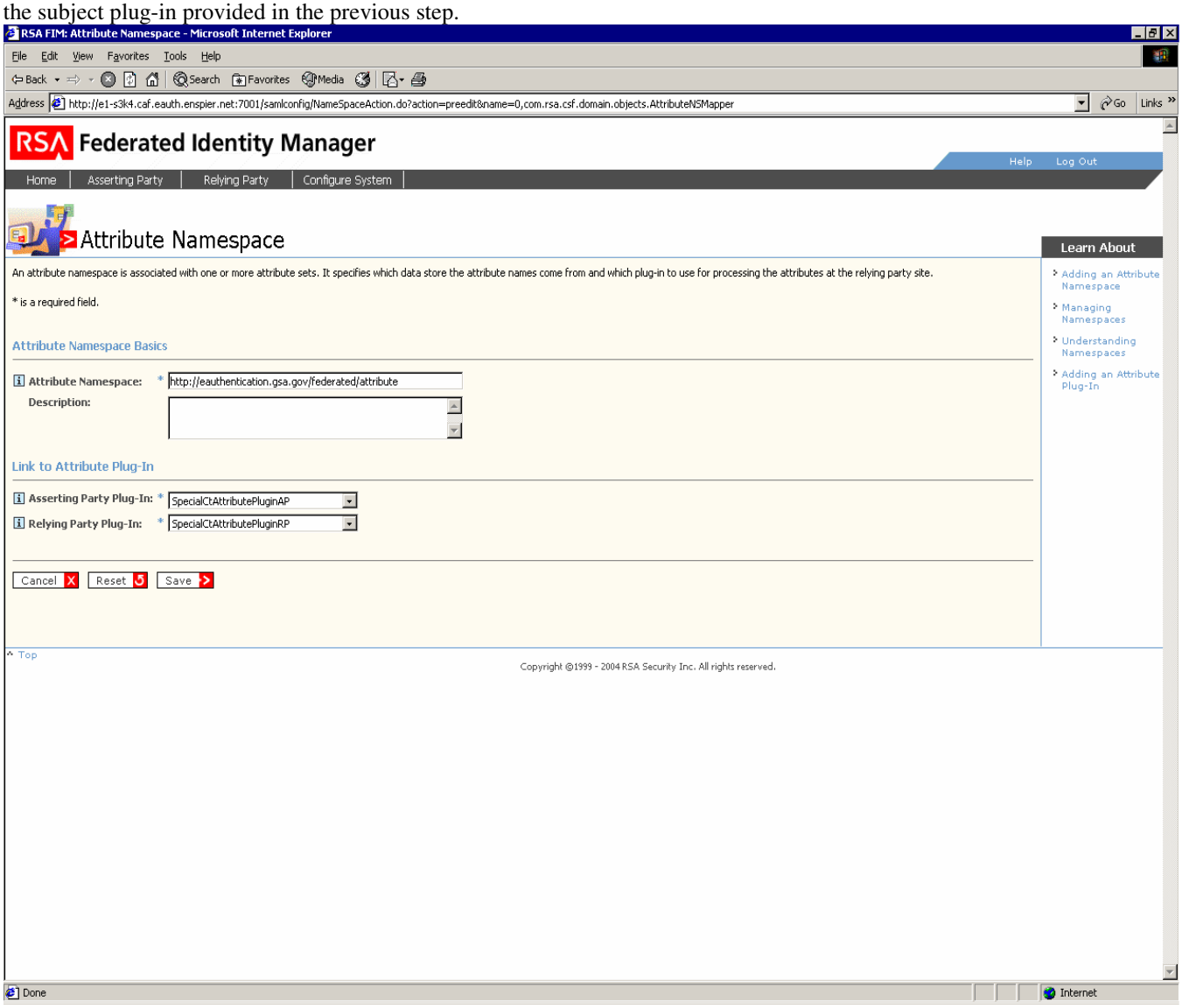

Figure 19-10: Attribute Namespace

For a CS in Asserting Party mode, a namespace corresponding to the value being sent in the namequalifier of the assertion must be created. This is linked to the subject plug-in provided in the previous step. An example of creating a subject namespace is provided in Figure 19-11.

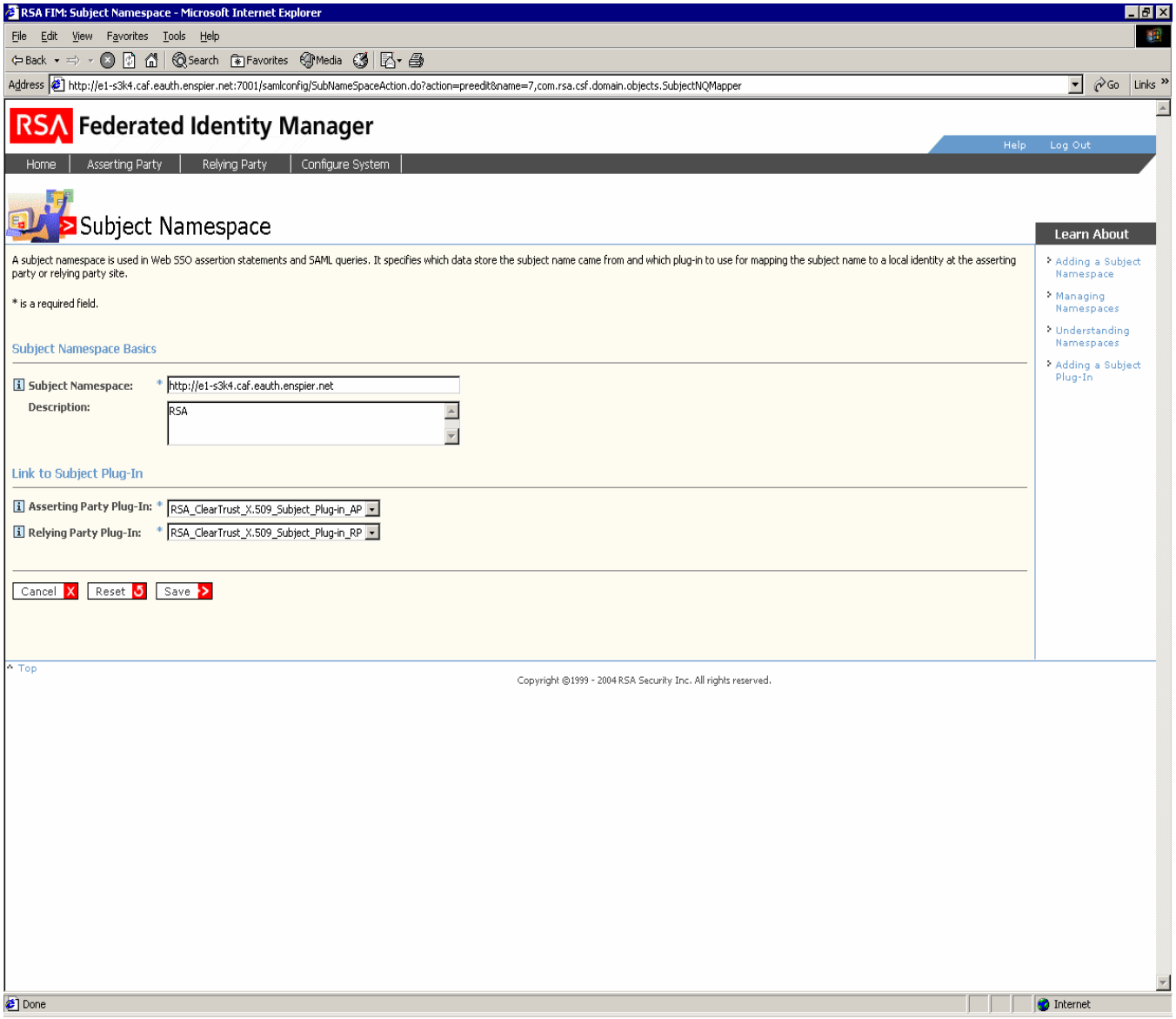

Figure 19-11: Subject Namespace

For an AA in Relying Party mode, a namespace corresponding to the asserting party's namequalifier from the assertion must be created. An example of creating this namespace is provided in Figure 19-12

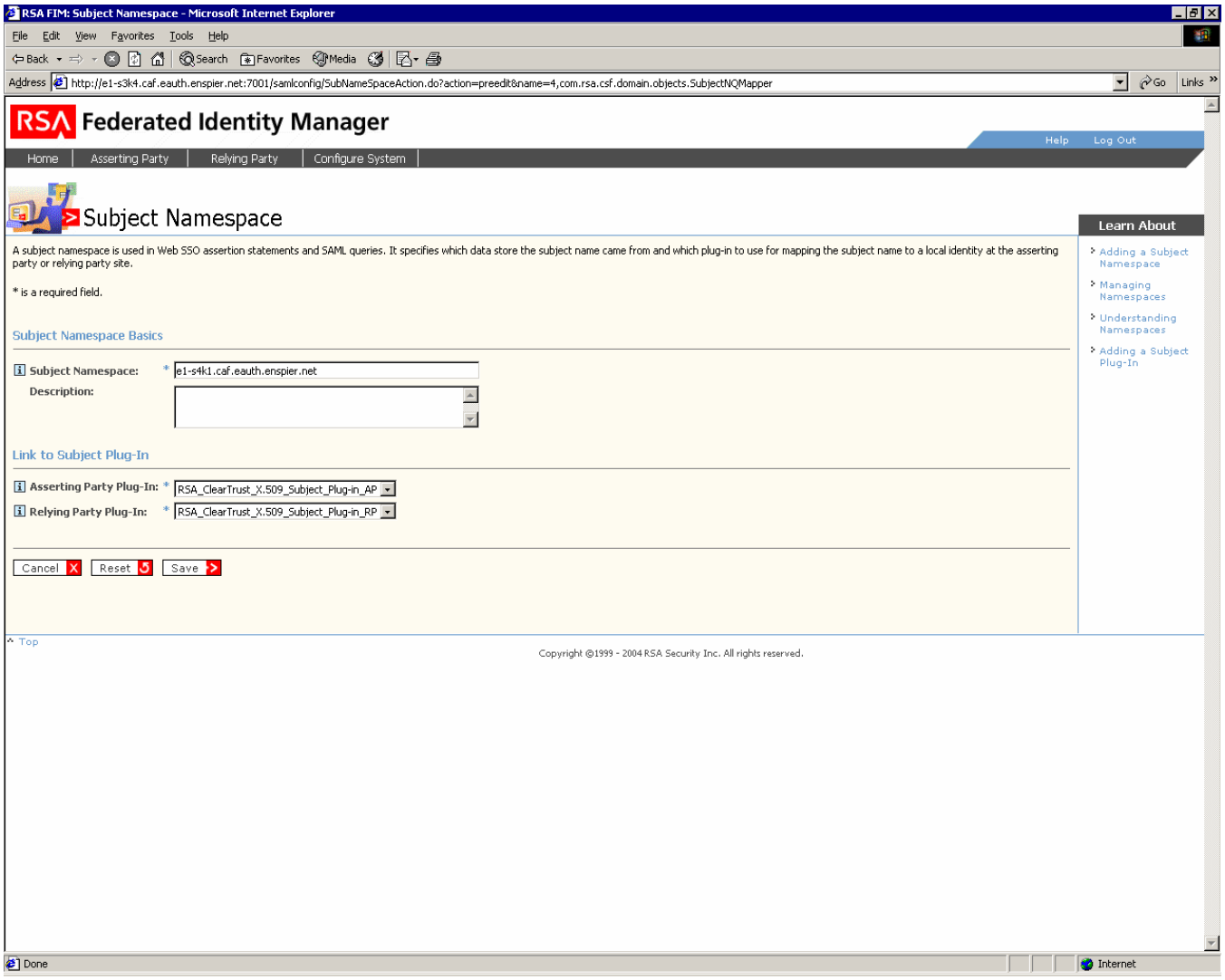

Figure 19-12: Namespace for an AA in Relying Party Mode

Next, attribute sets need to be configured. This is done by clicking on **Configure System > Attribute Sets**. The Attribute Sets screen should appear as shown in Figure 19-13. For a CS, this is where attribute sets that are sent in the assertion are configured. For an AA, this is where the attribute sets that will be received from SAML partners are configured.

Attribute sets can be viewed and edited by selecting an attribute set and clicking on **Edit,** which is found in the Edit column of the Attribute Sets table. An attribute set can be added by clicking on the **Add New** button provided above the Attribute Sets table.

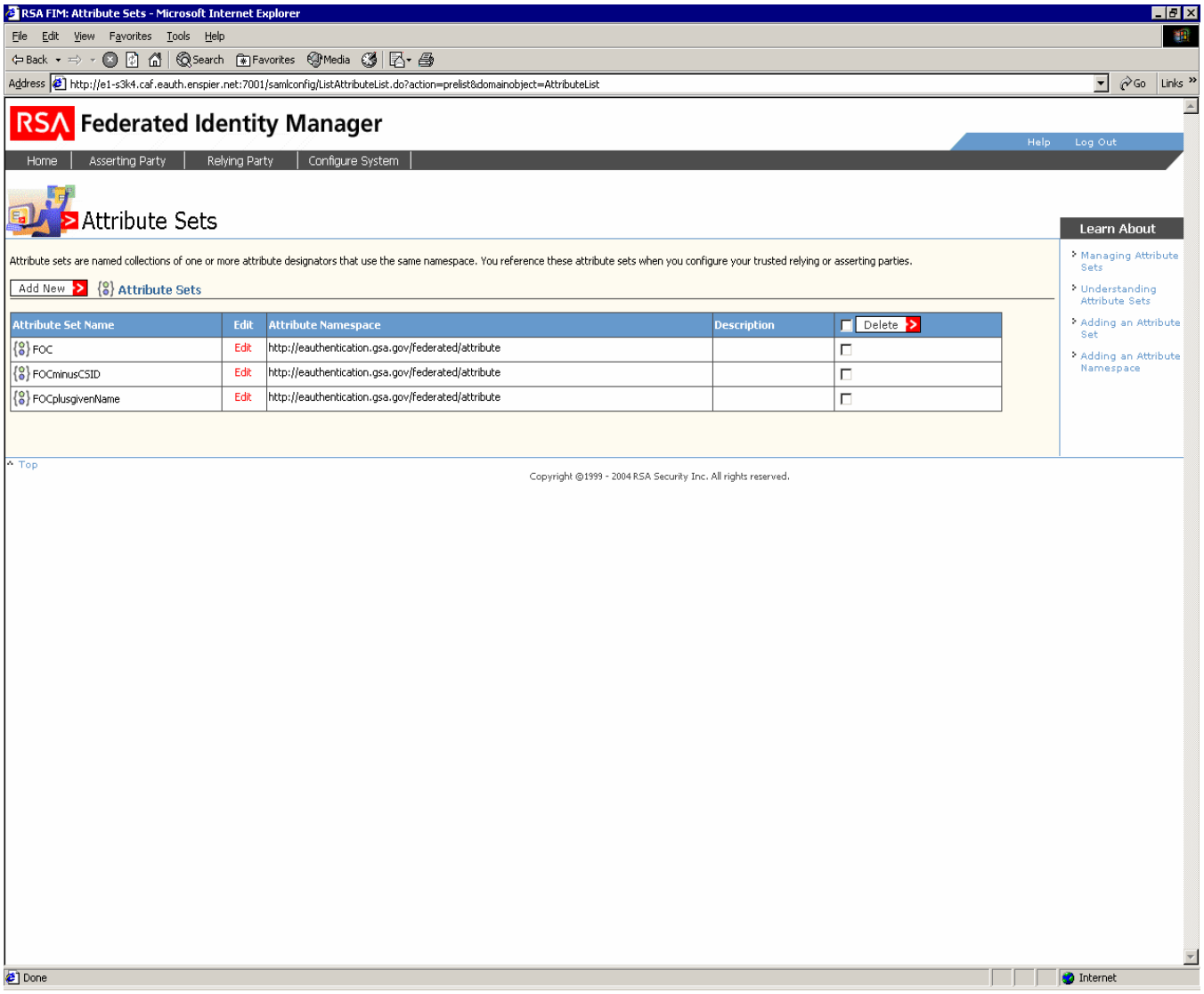

Figure 19-13: Attribute Sets

Figure 19-14 provides the properties of an attribute set. The names of the attributes are **assuranceLevel**, **CSid**, and **commonName**. These attributes correspond to user attributes provided in the SAML assertion and the LDAP user store.

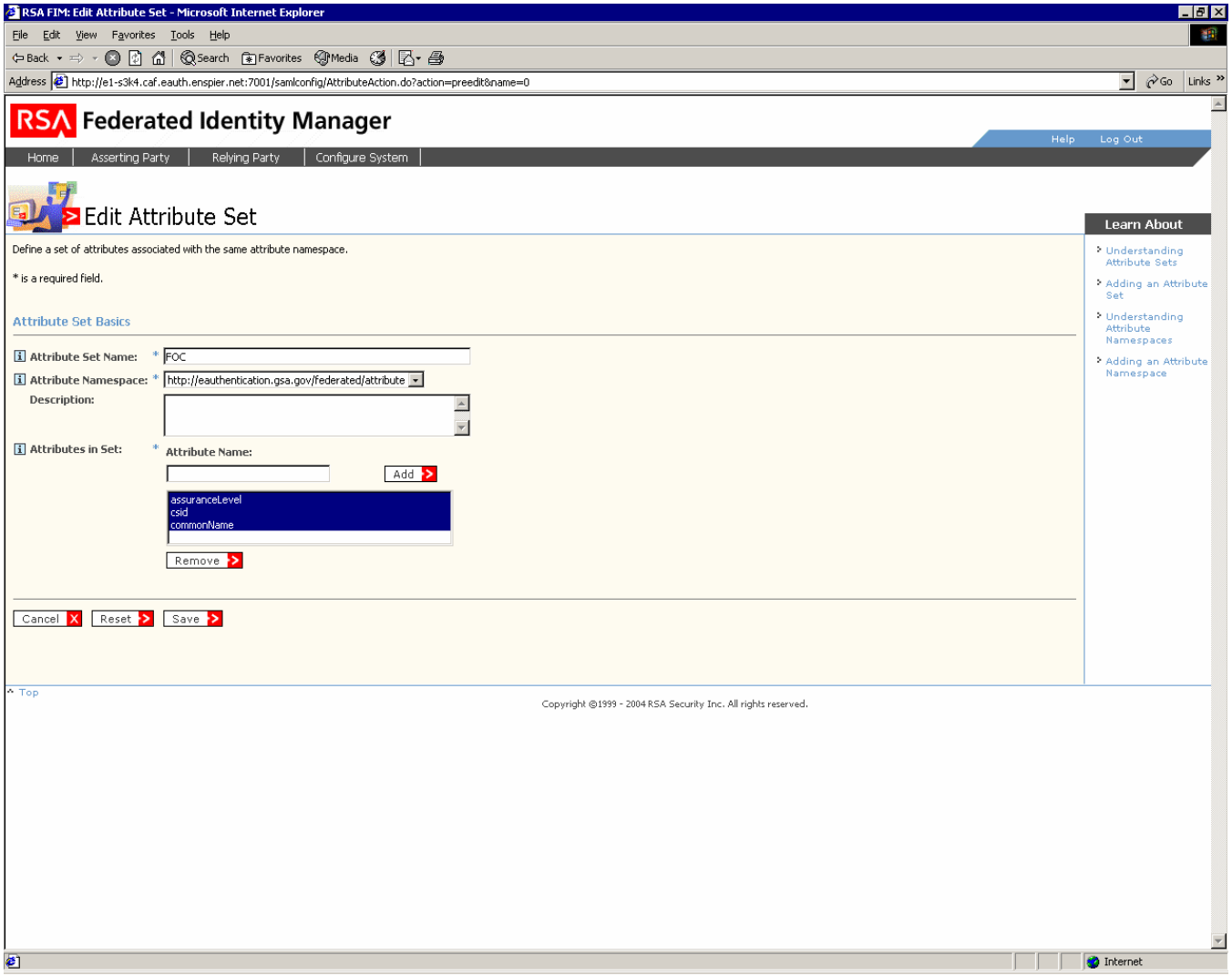

Figure 19-14: Edit Attribute Set

Next, keystores need to be configured. This is done by clicking on **Configure System > Keystores**. The Keystores screen will appear as shown in Figure 19-15. For a CS (AP mode), this is where a reference to a copy of your SAML partner client SSL certificate is created. For an AA (RP mode), this is where a reference to the client key that will be presented to your SAML provider will be created.

Keystores can be viewed and edited by selecting a namespace and clicking on **Edit,** which is found in the Edit column of the Keystore table. A new keystore can be added by clicking on the **Add New** button provided above the Keystore table.

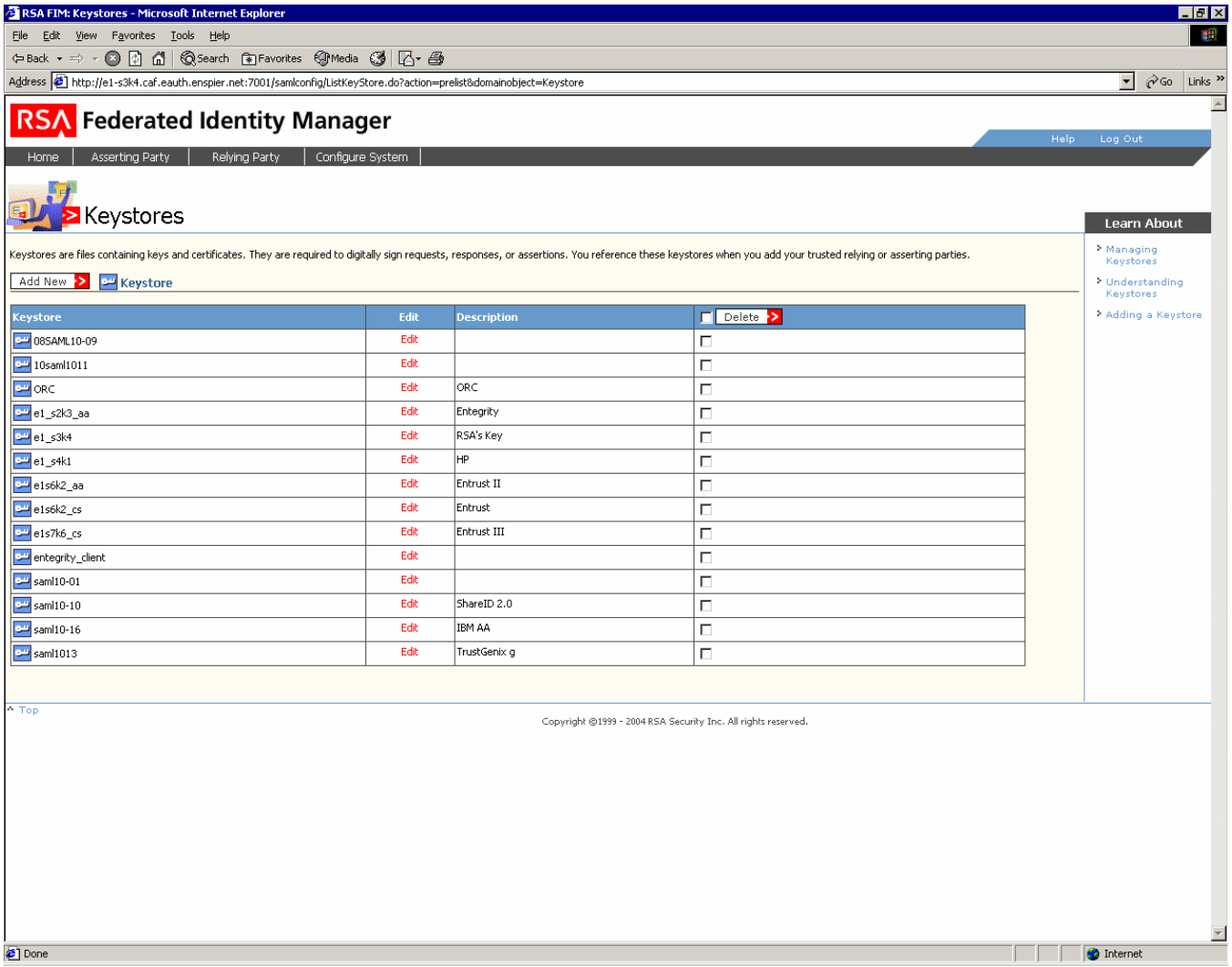

Figure 19-15: Keystores

For an AA's RSA client key, the **Keystore Path** and **Filename** field is the path to the java keystore where the client key pair is stored. The **Certificate Alias** is the alias in the keystore for the key pair. An AA must supply both the **Keystore Password** and **Private Key Password**. An example of this is provided in Figure 19-16.

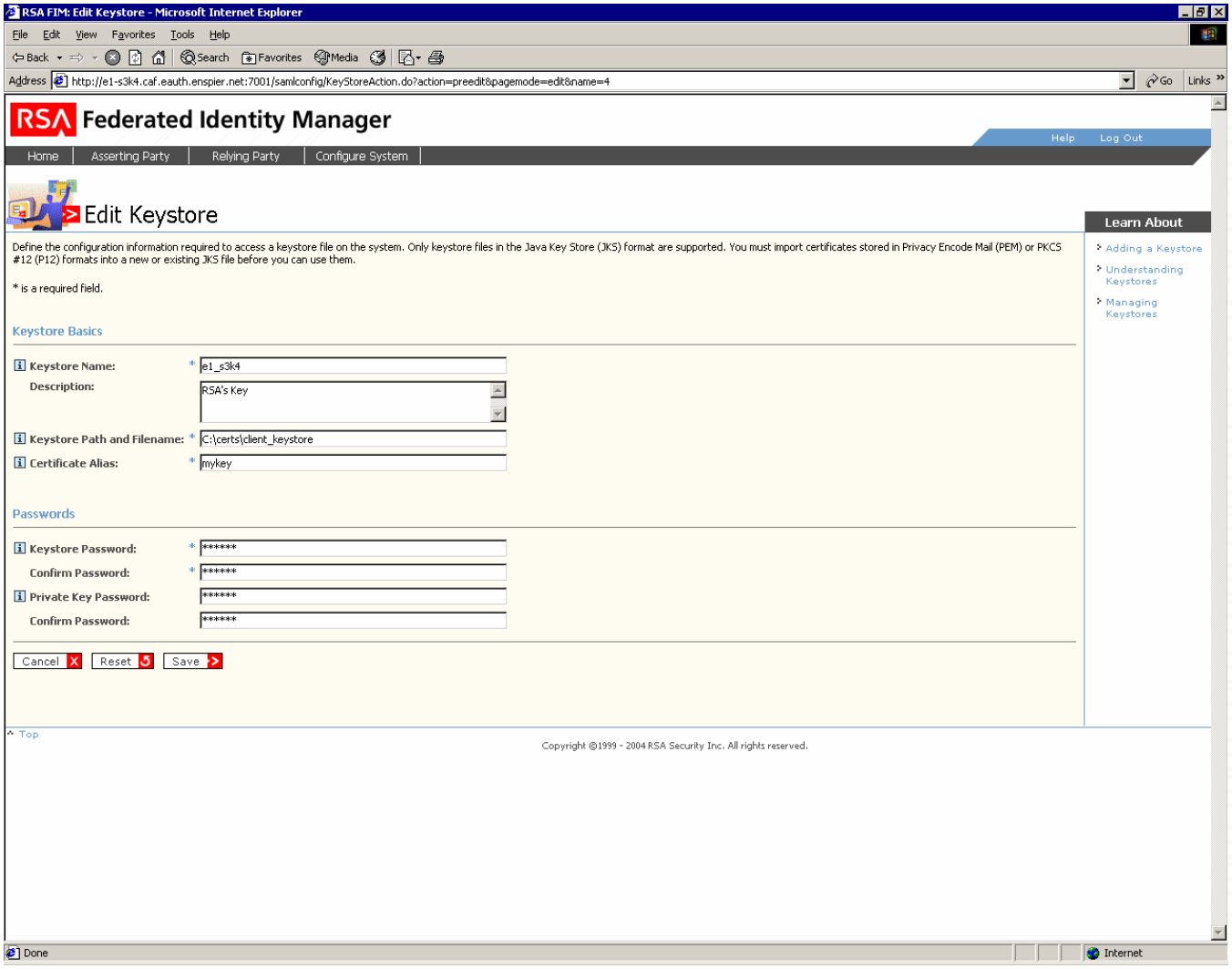

Figure 19-16: Edit Keystore

For a CS's SAML partner client SSL certificate, the **Keystore Path and Filename** field is the path to the java keystore where the SAML partner's public key is stored. The **Certificate Alias** is the alias in the keystore for the public key. For a CS, the **Keystore Password** must be supplied. An example of this is provided in Figure 19-17.

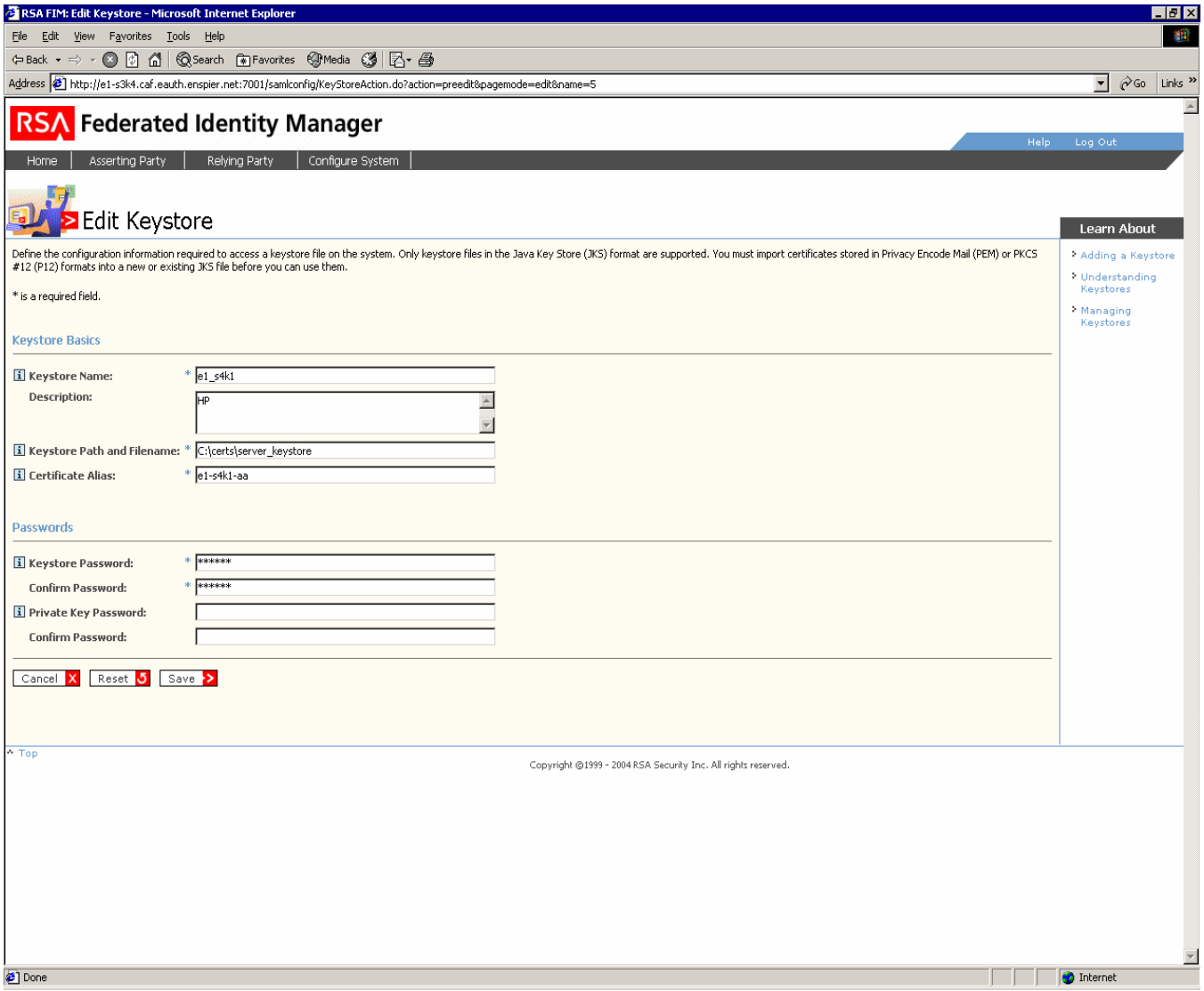

Figure 19-17: Keystore for a CS SAML Partner Client SSL Certificate

For a CS (AP mode), in addition to having a copy of the client's certificate, a user in WebLogic, with same name as the subject of the certificate, must be added. This is done by opening a web browser (i.e. Internet Explorer) and going to the WebLogic console (http://e1-s3k4.caf.eauth.enspier.net:7081/console). Once the WebLogic Server Console opens, select **csfdomain > Security > Realms > myrealm > Users** from the folder menu on the left side of the screen. The myrealm> User screen will appear as shown in Figure 19-18. Next, click on the **"Configure a new User"** link.

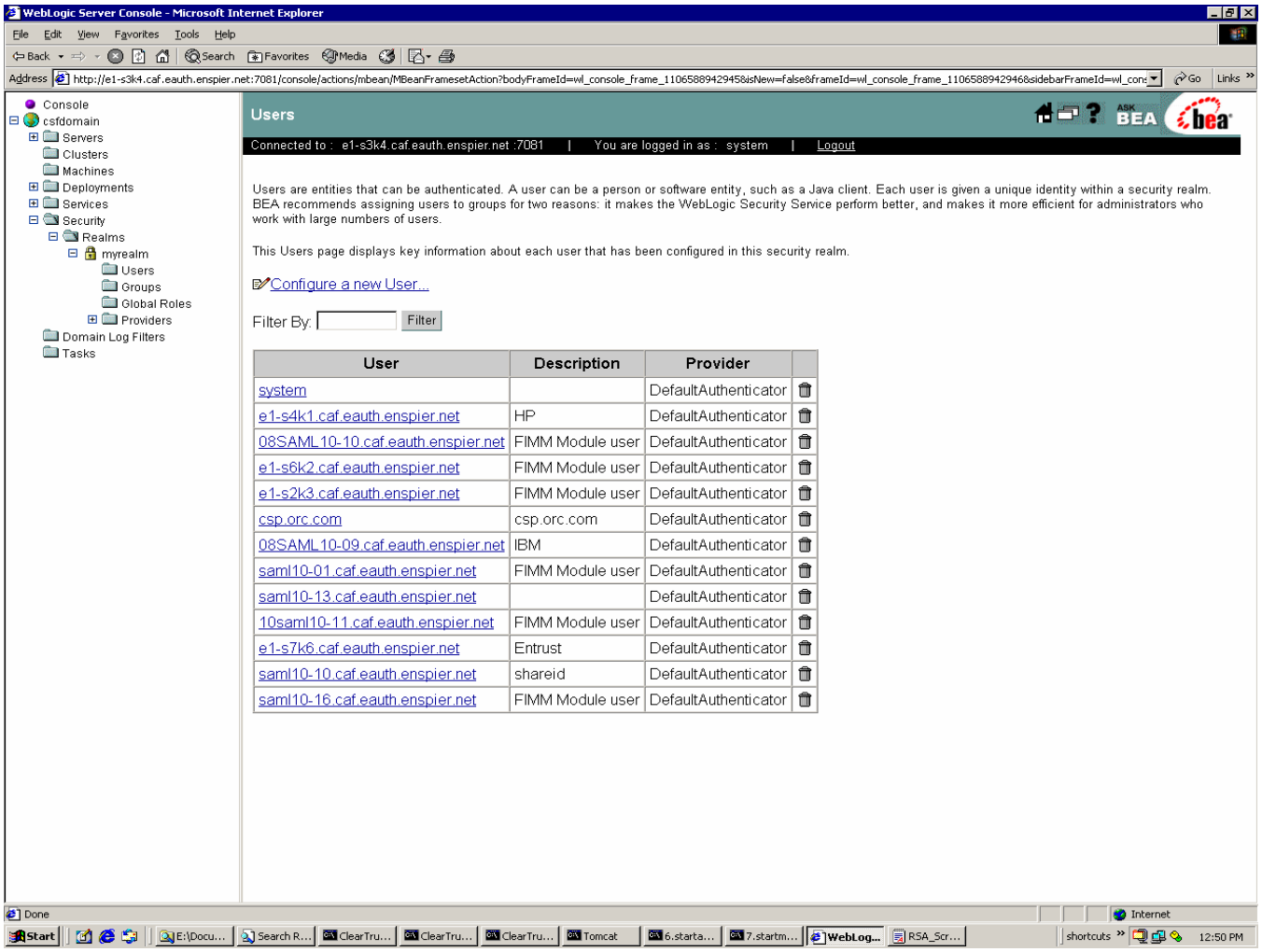

Figure 19-18: WebLogic Users

Once you click on the “Configure a New User” link, the myrealm>Create User screen should appear as shown in Figure 19-19. In the **Name** field, add a user whose username is the same as the CN in the Subject DN of the X.509 certificate and then click the **Apply** button.

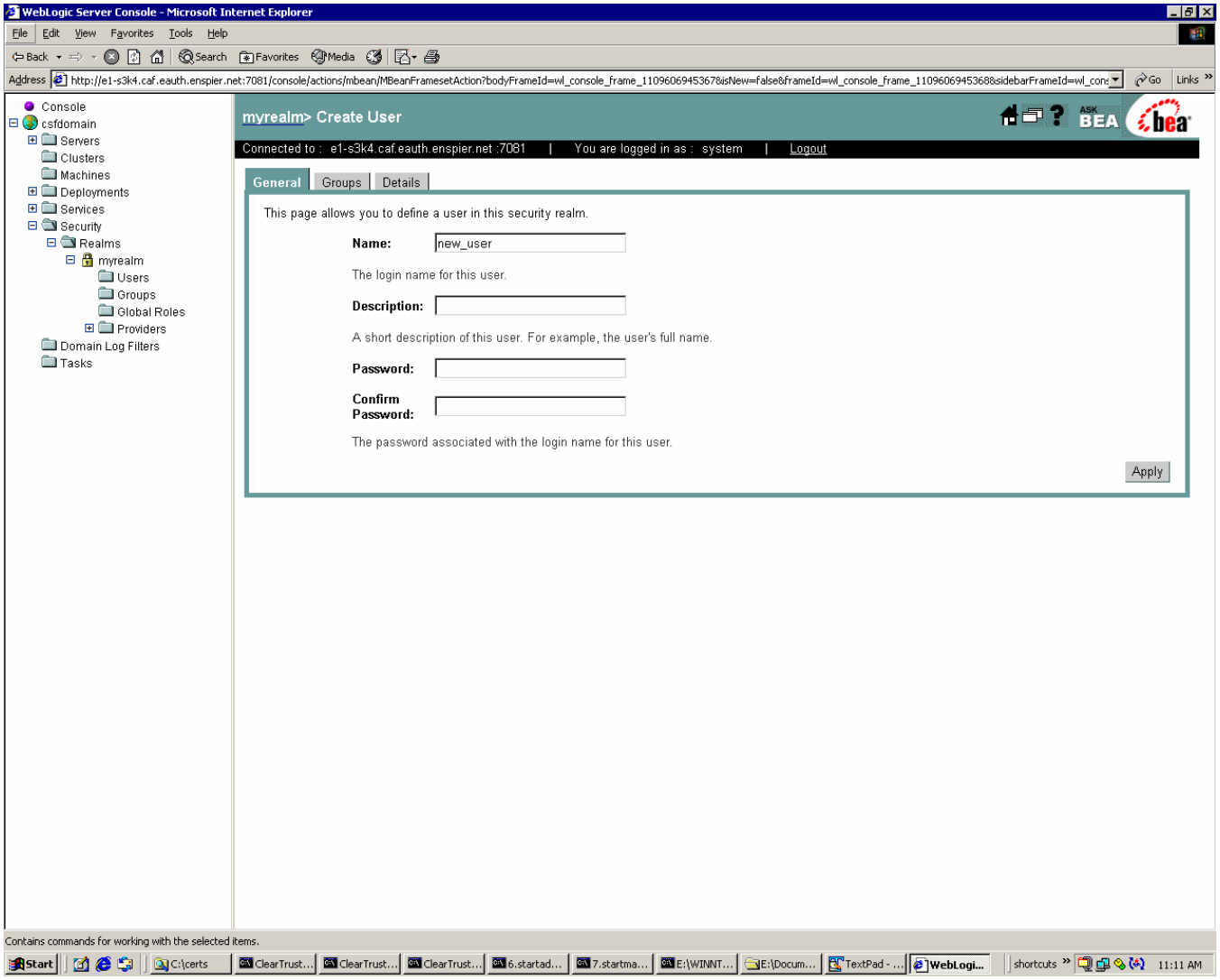

Figure 19-19: myrealm>Create User

Next, add the user created in the previous step to the SAMLBasicAuthUsers group. Click on the **Groups** tab, select the user from the **Possible Groups** column, and click on the → key. This will move the selected user to the **Current Groups** column. To conclude adding the user to the SAMLBasicAuthUsers group, click on the **Apply** button.

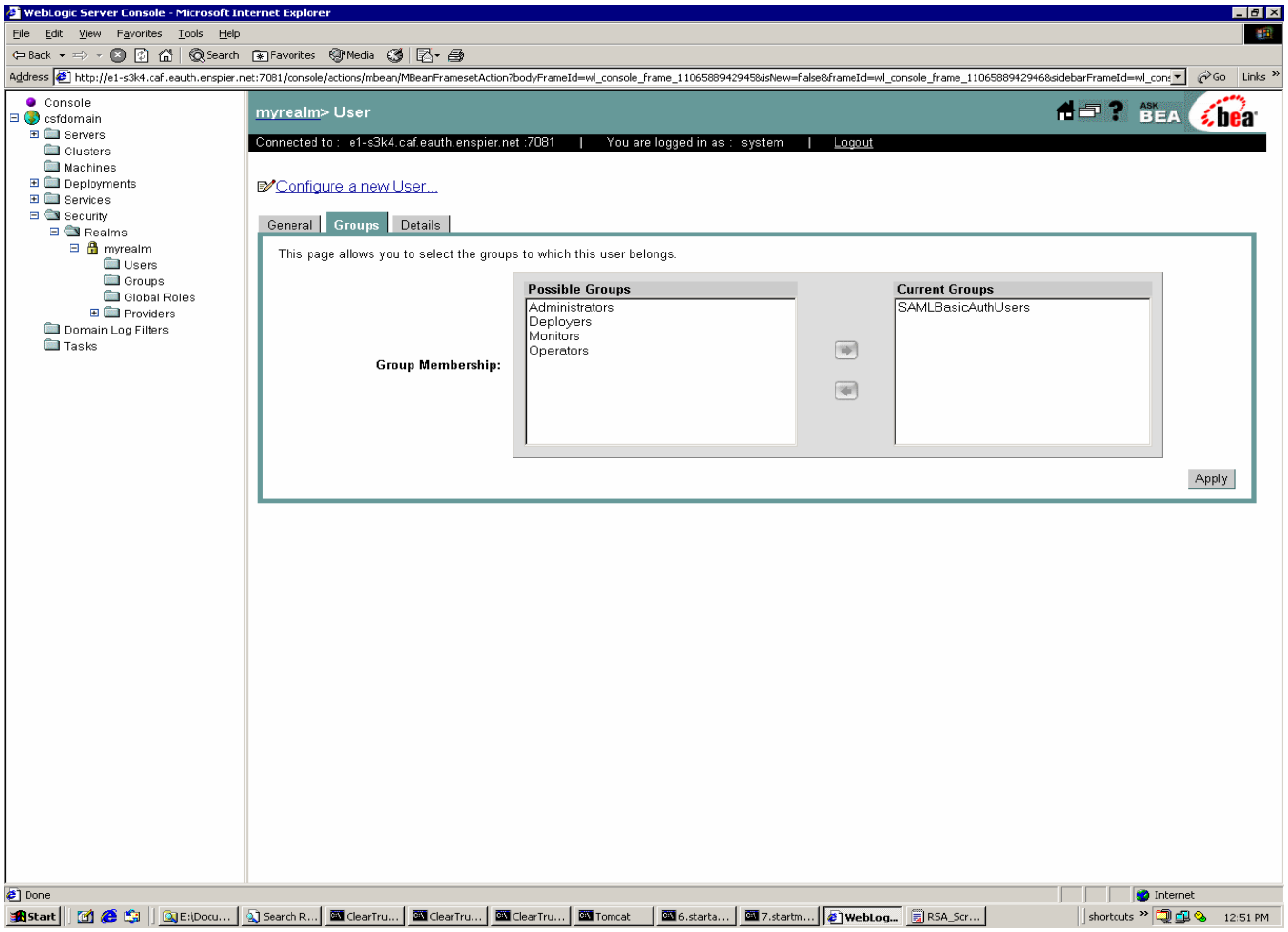

Figure 19-20: Add User to SAMLBasicAuthUsers Group

Next, verify that the SAMLBasicAuthUsers group is in the web.xml file. The web.xml file can be viewed by opening **Windows Explorer**. From the Windows Explorer folders menu, scroll down until you find **RSASecurity.** Open **RSASecurity > FIM25 > rsaappserver > config > csfdomain > applications > samlAssertingParty > WEB-INF** as demonstrated in Figure 19-21. Once the files stored in the WEB-INF appear, open the **web.xml** file.

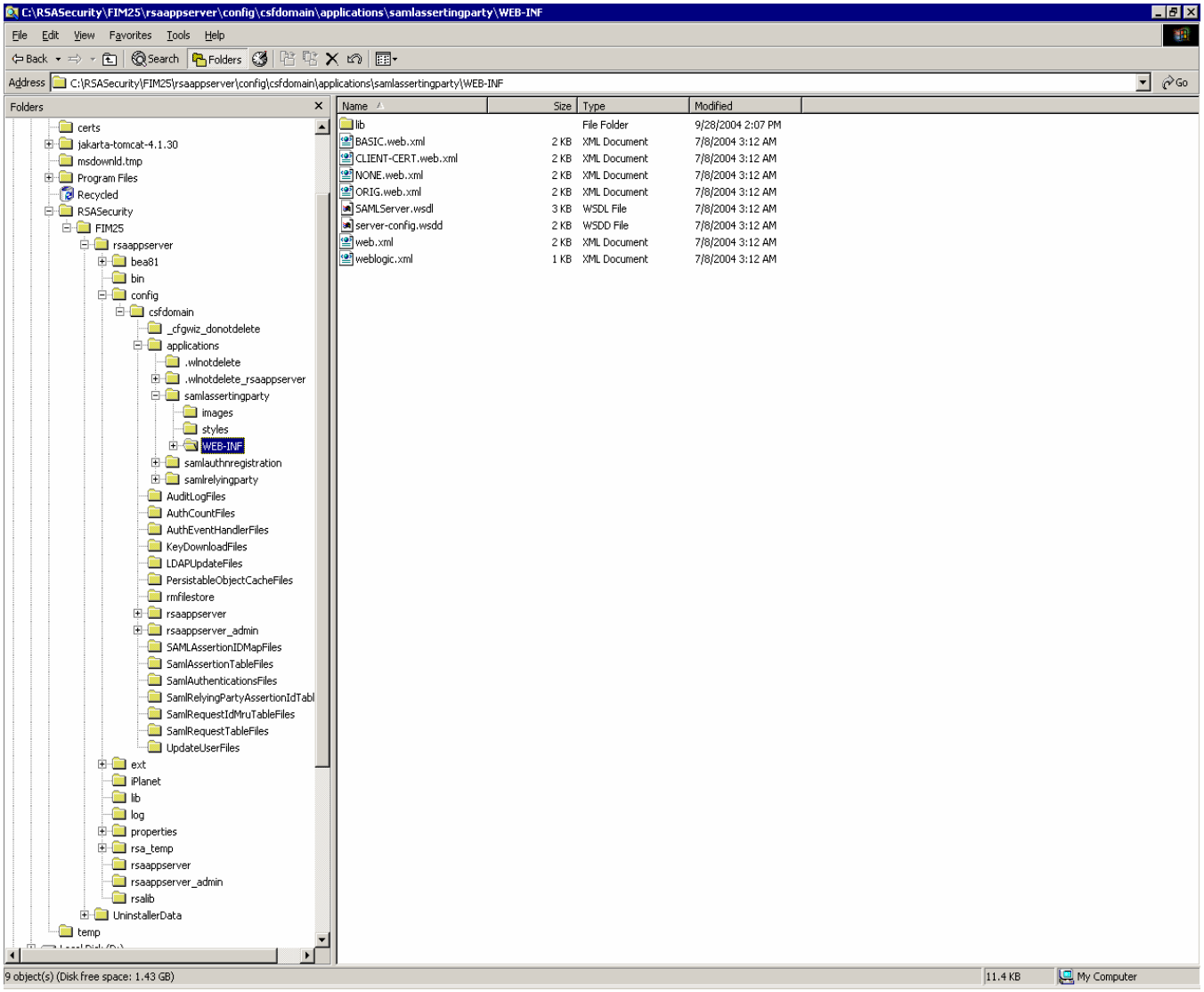

Figure 19-21: Verify SAMLBasicAuthUsers Group

The text in the web.xml should appear as provided below. Scroll through the text and search for **SAMLBasicAuthUsers**, which should appear as <role-name>**SAML_Basic_Auth_Users**</role-name>.

```
<?xml version="1.0"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
   "http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
        <display-name>SAML Asserting Party</display-name>
        <description>Servlets that provide SAML Asserting Party functionality</description>
        <servlet>
                <servlet-name>SamlSsoAssertingPartyServlet</servlet-name>
                <display-name>SAML SSO Asserting Party Servlet</display-name>
                <description>Servlet that provides SAML SSO Intersite Transfer Service (ISX)
functionality</description>
                <servlet-class>com.rsa.csf.application.saml.SamlSsoAssertingPartyServlet</servlet-class>
        </servlet>
        <servlet>
                <servlet-name>AxisServlet</servlet-name>
                <display-name>Apache-Axis Servlet</display-name>
                <servlet-class>org.apache.axis.transport.http.AxisServlet</servlet-class>
        </servlet>
        <servlet-mapping>
                <servlet-name>SamlSsoAssertingPartyServlet</servlet-name>
                <url-pattern>/AP/*</url-pattern>
        </servlet-mapping>
        <servlet-mapping>
                <servlet-name>AxisServlet</servlet-name>
                <url-pattern>/services/*</url-pattern>
        </servlet-mapping>
        <welcome-file-list>
                <welcome-file>index.html</welcome-file>
        </welcome-file-list>
        <!-- Authentication -->
        <security-constraint>
                <web-resource-collection>
                        <web-resource-name>SAML Request</web-resource-name>
                        <url-pattern>/services/SamlRequest</url-pattern>
                </web-resource-collection>
                <auth-constraint>
                        <role-name>SAML_Basic_Auth_Users</role-name>
                </auth-constraint>
        </security-constraint>
        <login-config>
                <auth-method>CLIENT-CERT</auth-method>
        </login-config>
        <security-role>
                <role-name>SAML_Basic_Auth_Users</role-name>
        </security-role>
</web-app>
```

2.3 Configure a Partner AA

From the RSA Federated Identity Manager home screen, click on **Asserting Party > Trusted Relying Parties > Add New**. The Add Trusted Relying Party screen will appear as shown in Figure 19-22. From this screen, select **Specify all the settings yourself** option and select the **Next** button at the bottom of the screen.

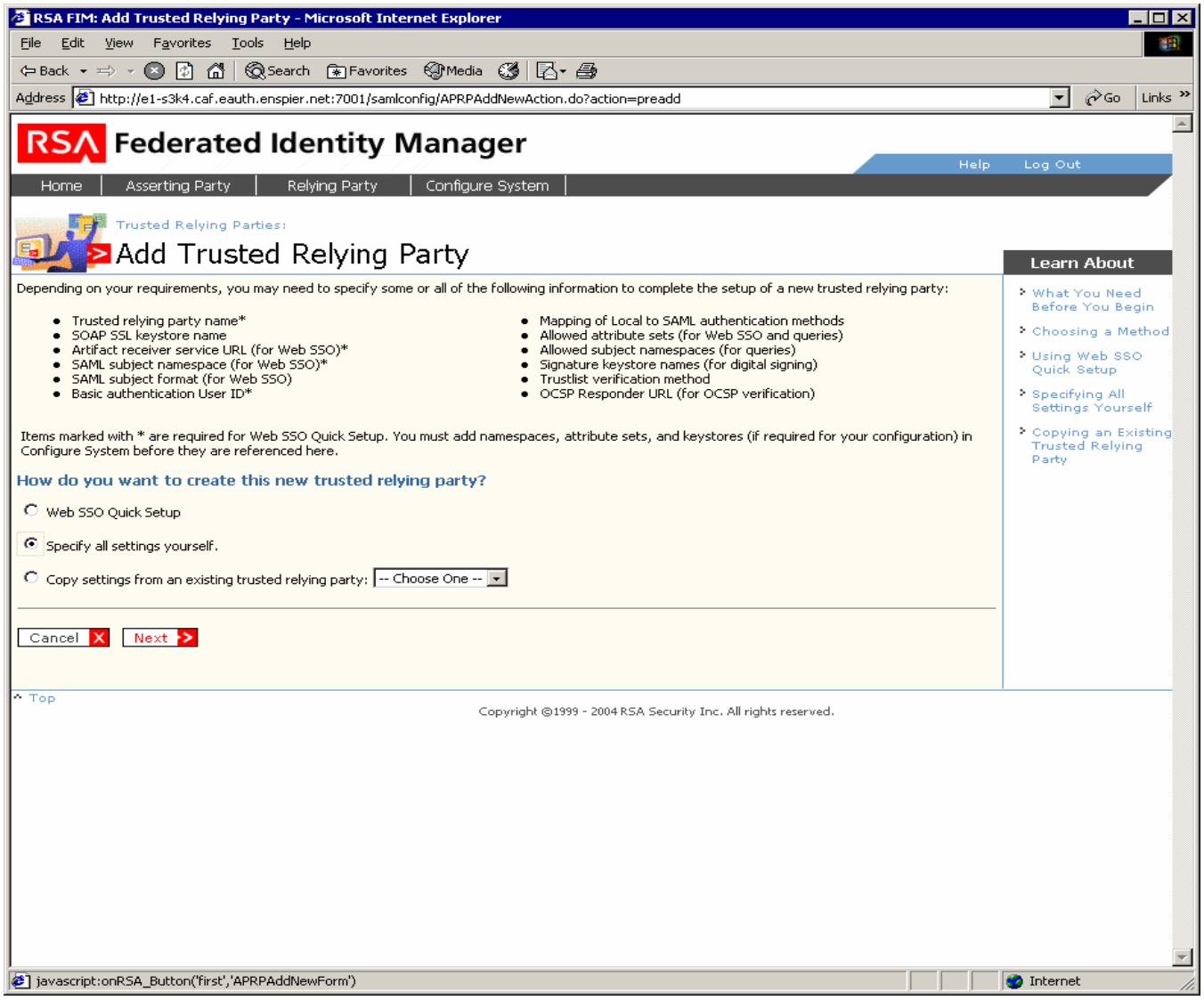

Figure 19-22: Add Trusted Relying Party

Next, the Add Trusted Relying Party – Basics screen will appear as shown in Figure 19-23. Enter all the appropriate configuration information as demonstrated below. The **SOAP SSL Keystore** value was predefined in a previous step (Figure 19-15). This is a reference to the SAML partner's public key which will be presented when requesting an assertion. Once all configuration information has been provided, select the **Next** button at the bottom of the screen.

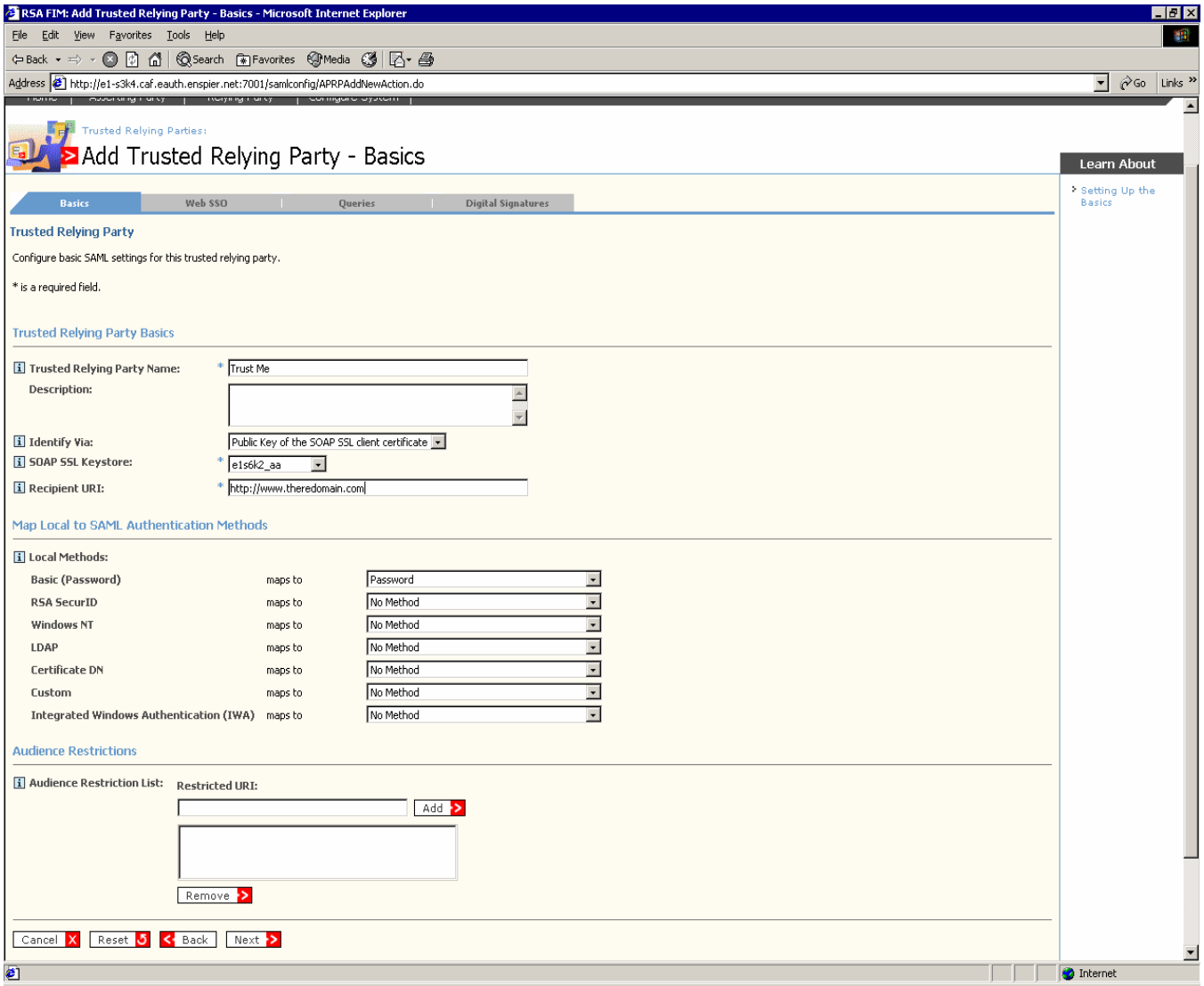

Figure 19-23: Add Trusted Relying Party - Basics

Next, the Add Trusted Relying Party – Web SSO screen will appear as shown in Figure 19-24. Enter all appropriate configuration information as demonstrated below. The Subject Namespace and Attribute Statement refer to what you will send to this partner in your assertion, which were predefined in previous steps (Figure 19-9). Once all configuration information has been provided, select the **Next** button at the bottom of the screen.

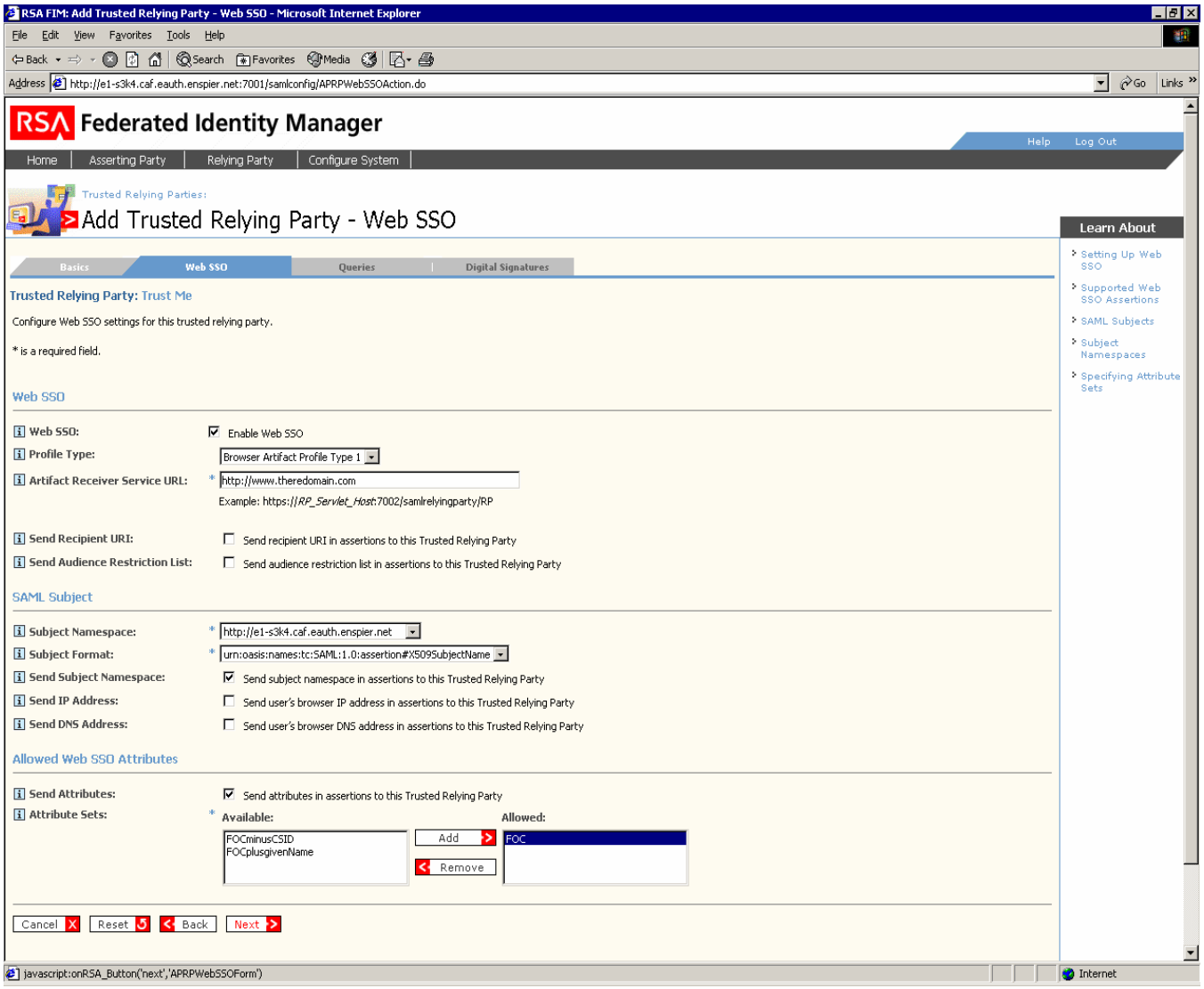

Figure 19-24: Add Trusted Relying Party – Web SSO

Next, the Add Trusted Relying Party – Queries screen will appear as shown in Figure 19-25. From the Queries section, be sure not to select **Enable attribute and authentication queries** option as demonstrated below. Select the **Next** button at the bottom of the screen.

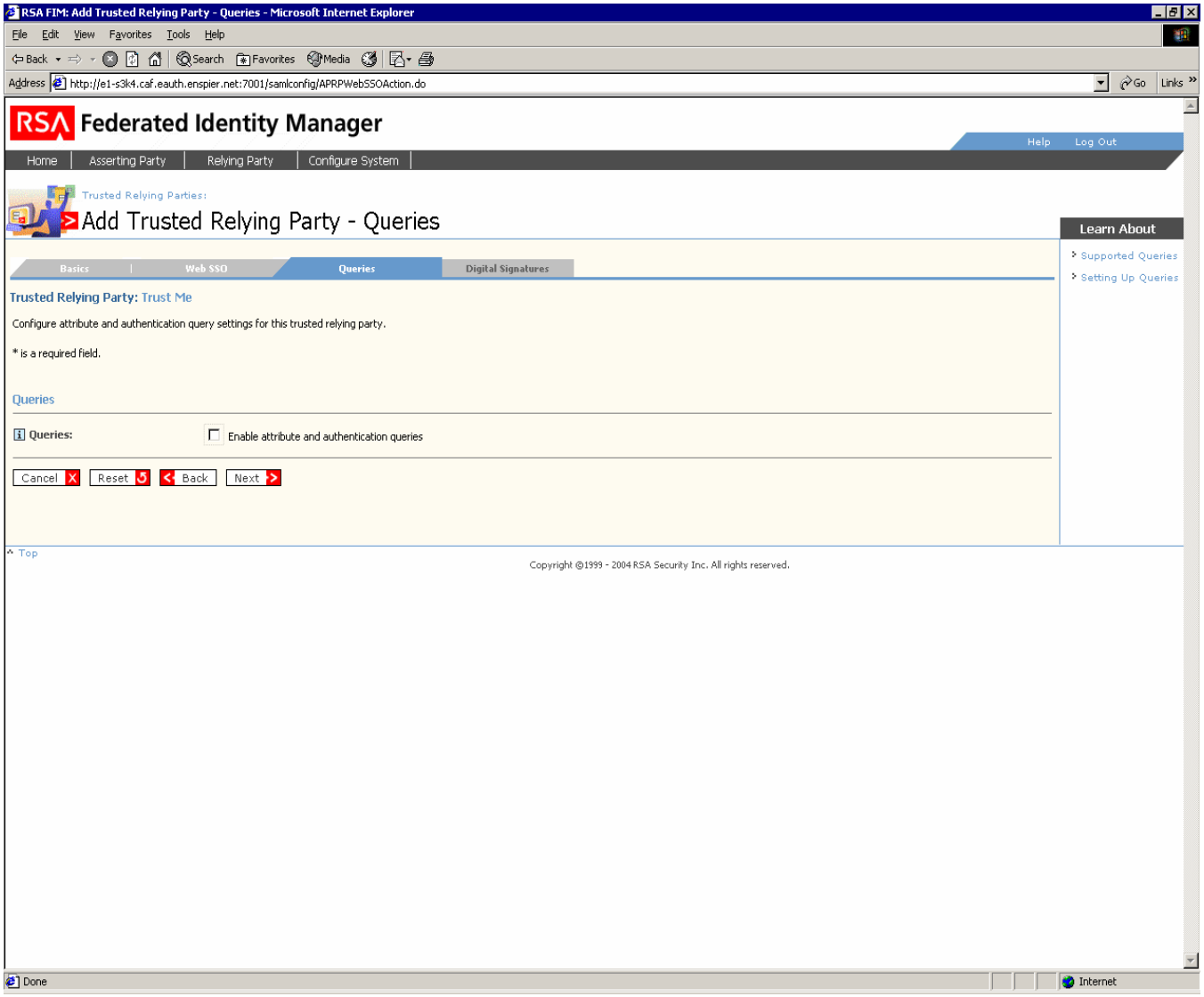

Figure 19-25: Add Trusted Relying Party – Queries

Next, the Add Trusted Relying Party – Signatures screen will appear as shown in Figure 19-26. Select all defaults as demonstrated below. Once all defaults have been selected, select the **Save** button at the bottom of the screen. This concludes the configuration of an AA partner.

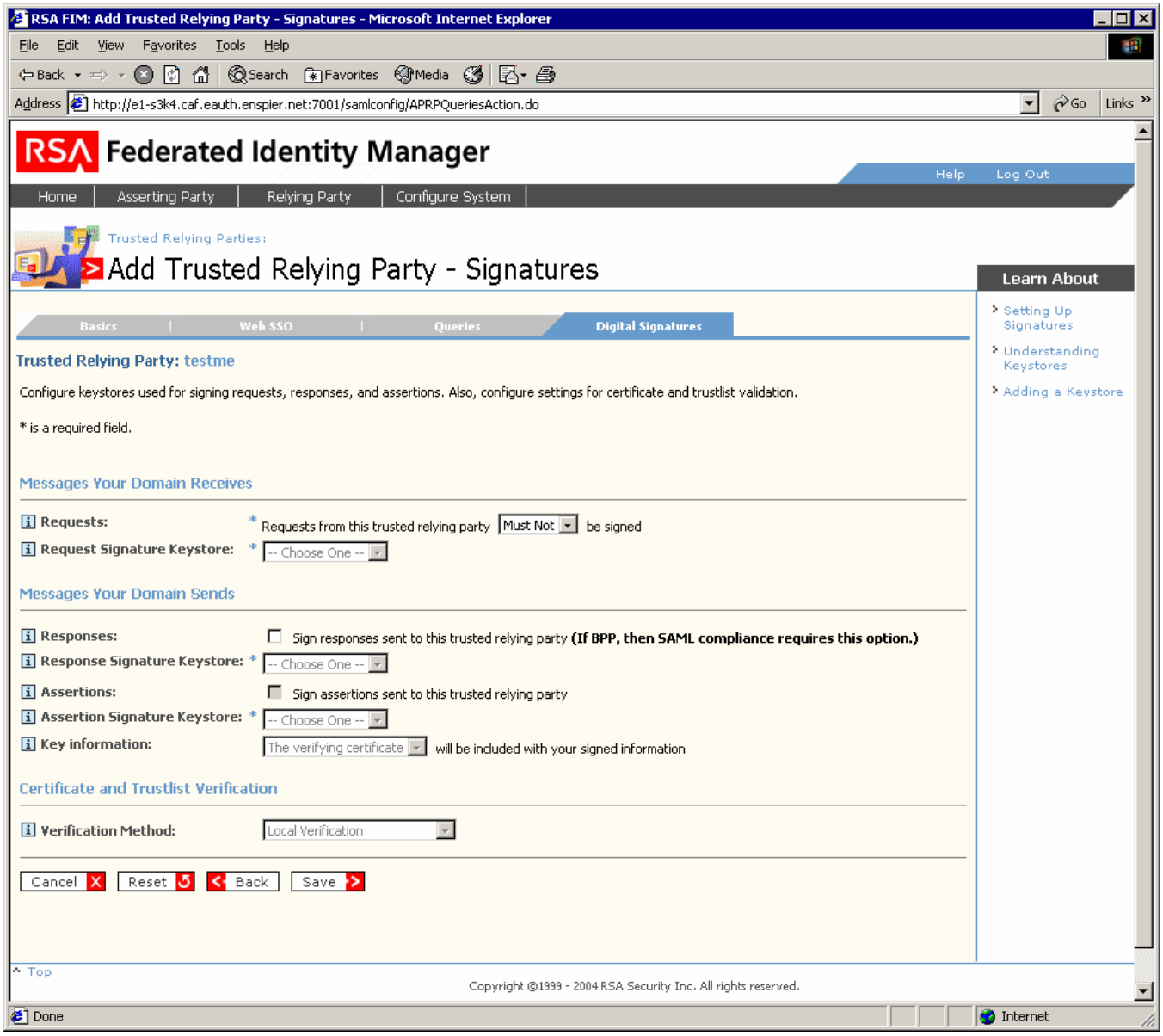

Figure 19-26: Add Trusted Relying Party - Signatures

2.4 Configure a Partner CS

From the RSA Federated Identity Manager home screen, click on **Relying Party > Trusted Asserting Party > Add New**. The Add Trusted Asserting Party screen will appear as shown in Figure 19-27. Once the screen appears, select **Specify all settings yourself** option and select the **Next** button at the bottom of the screen.

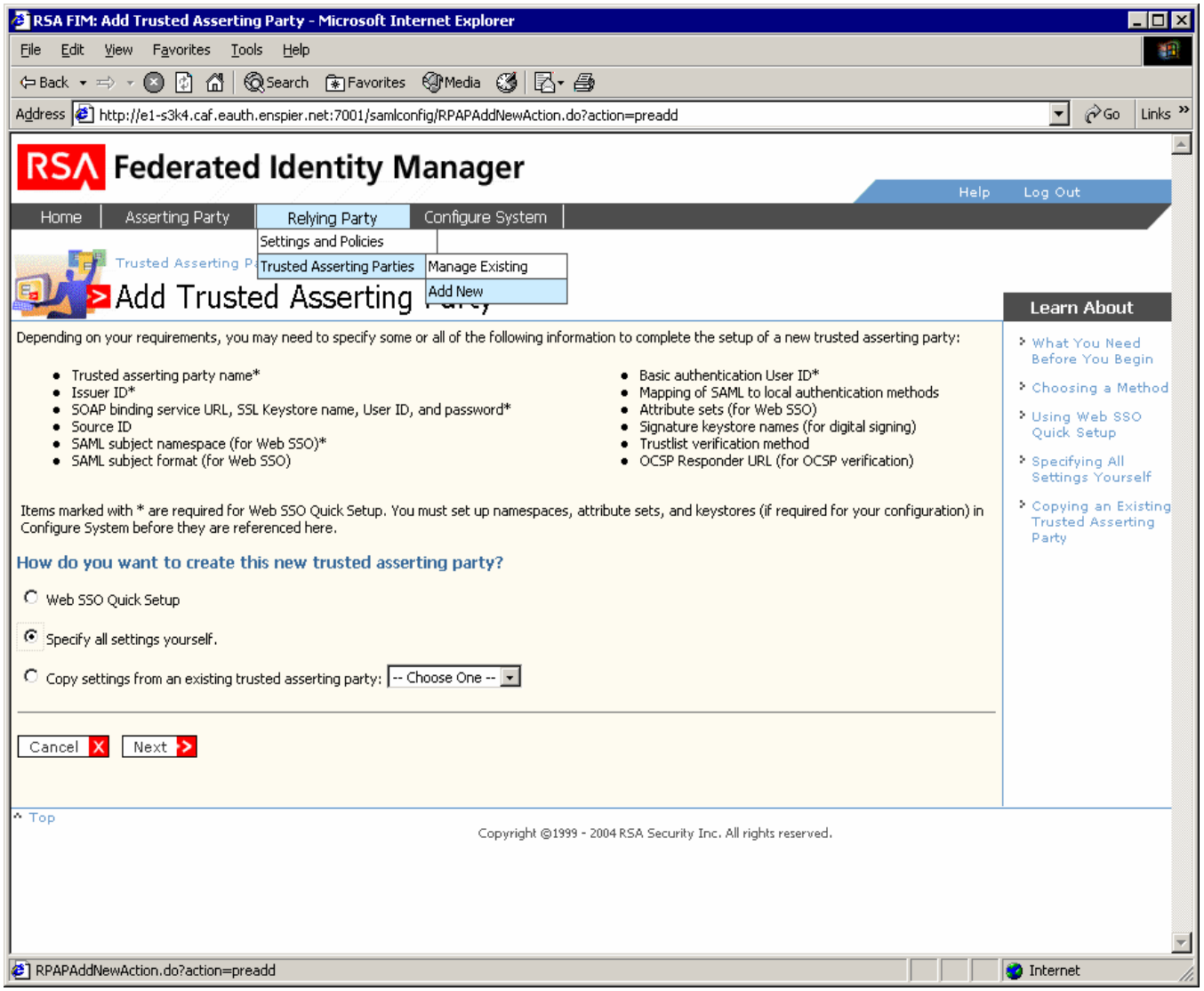

Figure 19-27: Add Trusted Asserting Party

Next, the Add Trusted Asserting Party – Basics screen appears as shown in Figure 19-28. Enter all the appropriate configuration information as demonstrated below. Be sure that the **Source ID** is a SHA1 hash of the Issuer ID. In addition, make sure you place the reference of the key pair in the **SOAP SSL Keystore** field. Once all appropriate information has been provided, select the **Next** button at the bottom of the screen.

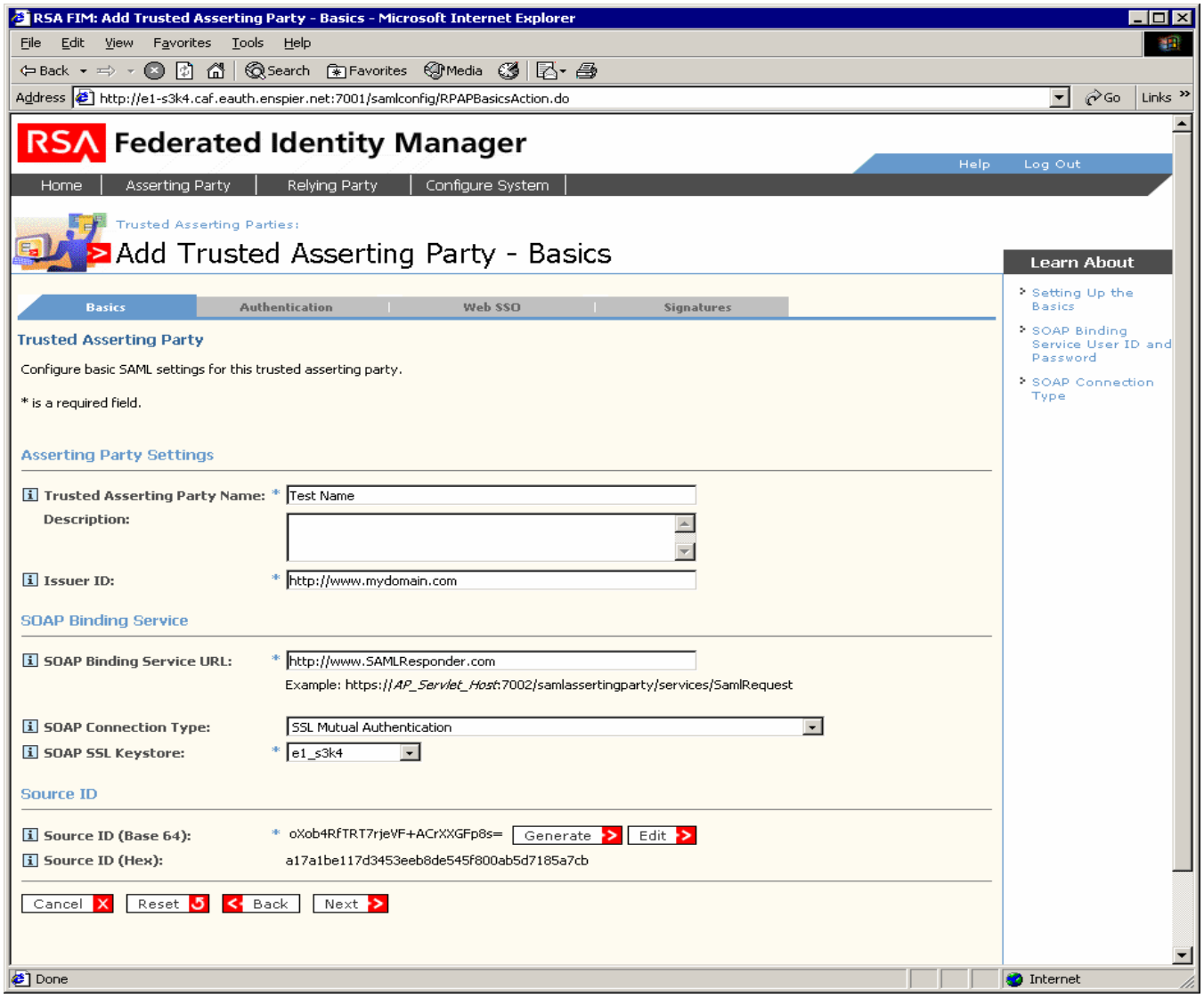

Figure 19-28: Add Trusted Asserting Party - Basics

Next, the Add Trusted Asserting Party – Authentication screen will appear as shown in Figure 19-29. As demonstrated below, select all the defaults and click on the **Next** button at the bottom of the screen.

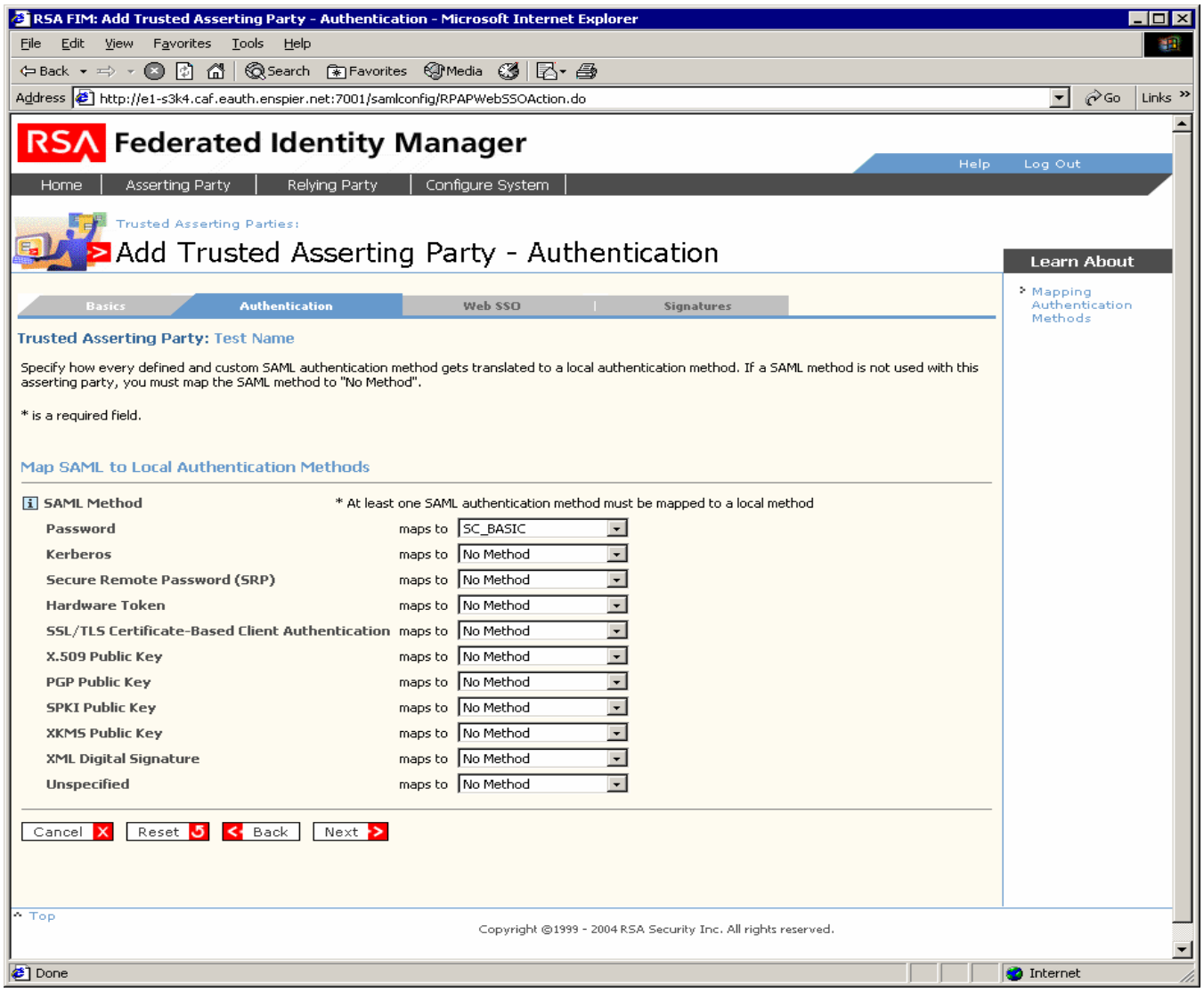

Figure 19-29: Add Trusted Asserting Party - Authentication

Next, the Add Trusted Asserting Party – Web SSO screen will appear as shown in Figure 19-30. Select and enter all appropriate configuration information as demonstrated below. The **Subject Namespace** corresponds to the namequalifier in the assertion that will be received from this partner, and the **Attribute Sets** are those that the sender will include in the assertion. Both of these must be included in the assertion that is received and are predefined under the Configure System options previously described (Figure 19-13). Once all appropriate configuration information has been provided, select the **Next** button at the bottom of the page.

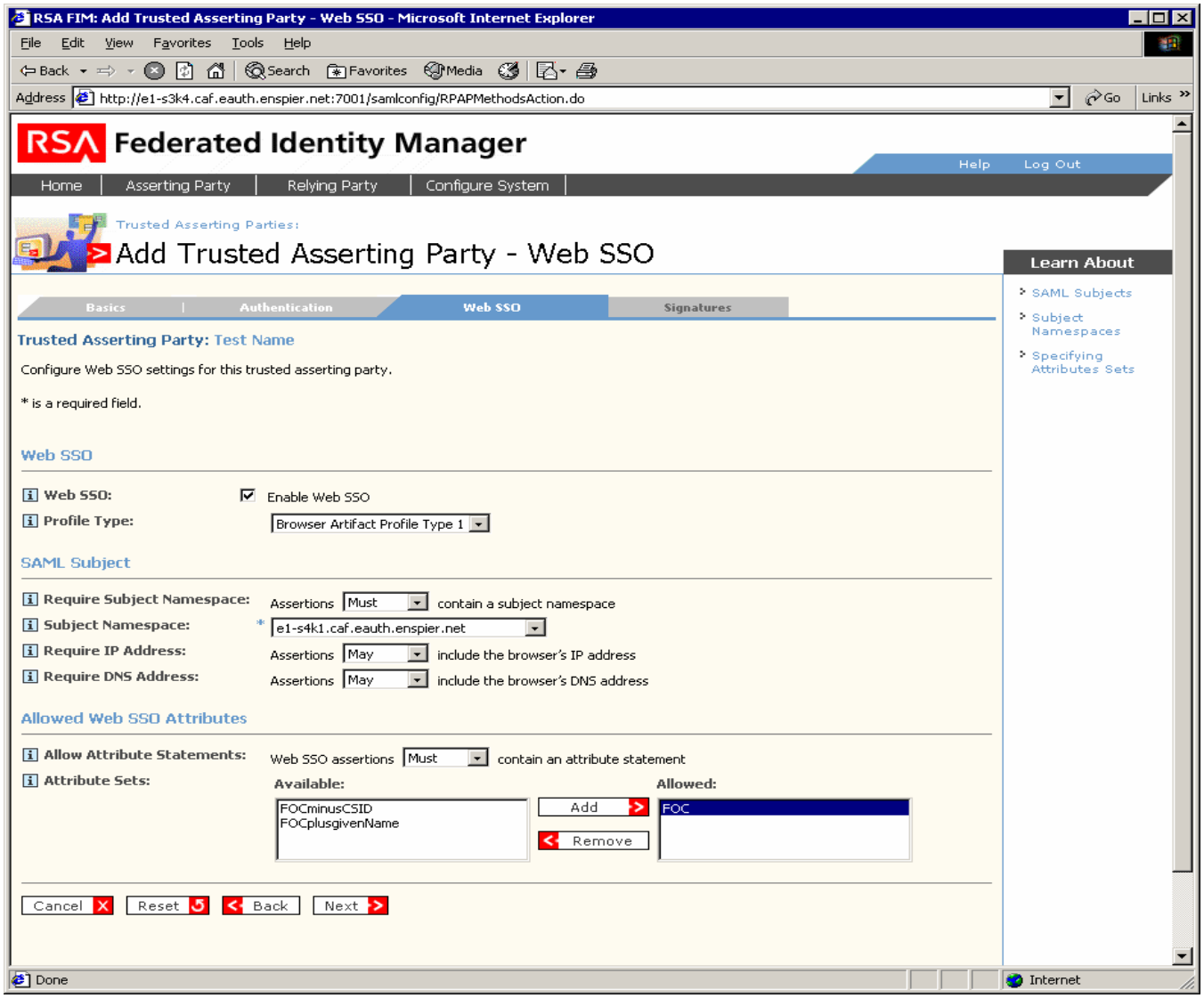

Figure 19-30: Add Trusted Asserting Party – Web SSO

Next, the Add Trusted Asserting Party – Signatures screen will appear as shown in Figure 19-31. Select all defaults as demonstrated below. Once all defaults have been selected, select the **Save** button at the bottom of the screen. This concludes the configuration of a CS partner.

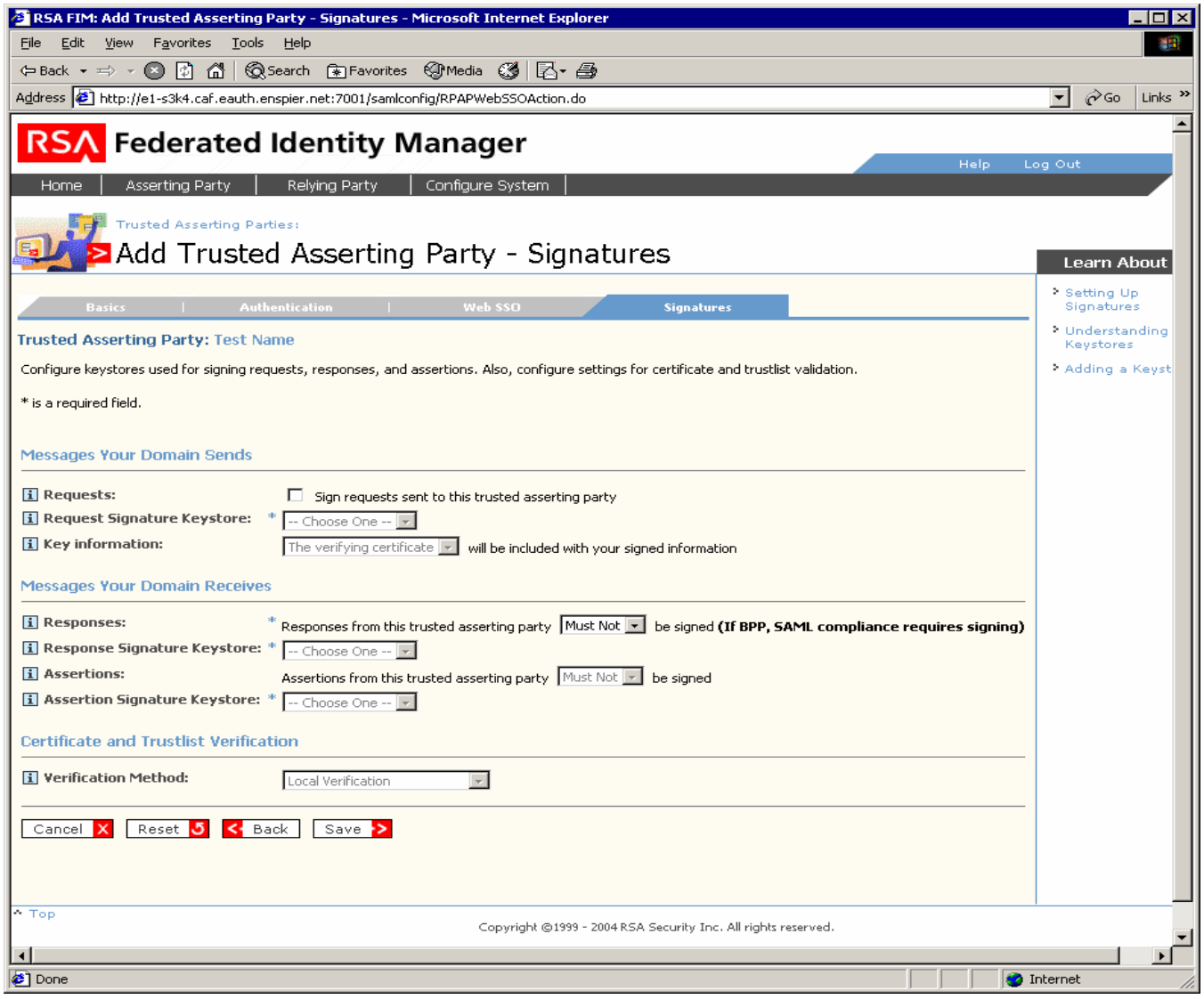

Figure 19-31: Add Trusted Asserting Party - Signatures